Enterprise Cloud

Functional Description

[Global Standard Services]

NTT Communications

Ver.2.36

(March 23th, 2015 Edition)

About This Document

[Structure of This Document]

The document is composed of three parts.

Overview part	1 Overview of the Enterprise Cloud
Features part	2 Service Management (Portal Site) 3 Compute (Global Standard Menu) 4 Backup (Global Standard Menu) 5 Network (Global Standard Menu) 6 External Storage (Global Standard Menu) 7 Security (Global Standard Menu) 8 Services Specific to Japan Data Centers (Local Option Menu)
Maint. part	9 Maintenance and Operation of the Enterprise Cloud (Japan Contract)

[Purpose of This Document/How to Use This Document]

This document explains the menus in the Enterprise Cloud and the features in each menu. Please note that the information in this document is for users who have signed contracts.

- If anything in the document is unclear, please contact an NTT sales representative or Support. The contact information for Support is included in this document.
- For instructions on how to use the Customer Portal, refer to "Enterprise Cloud User's Guide."
- The service may differ from the information in this document as a result of feature additions/changes. You can download the latest version of this document and user guides from the website below. You will need the ID/password provided when you started the service, or sent separately, to access and use the service.

  Support site for users with an Enterprise Cloud contract

  http://www.ntt.com/bhec/data/support.html

Contents

About This Document 2

Contents 3

1. Overview of the Enterprise Cloud 9

1.1 What is Enterprise Cloud? 9

1.2 Features that make up Enterprise Cloud 10

1.3 Services Available at All Data Centers (Global Standard Menu) 13

1.3.1 Available Equipment Environment 17

1.3.2 Available Data Centers 21

1.3.3 Service Order, Delivery Time and Minimum Usage Period 24

1.3.4 Resource Contract Conditions and Service Combination Conditions 30

1.4 Services That Have Data Center-Specific Usage (Local Option Menu) 32

1.5 Example Usage Model 34

1.6 Explanation of Common Terms 36

1.7 Restrictions 39

2. Service Management (Portal Site) 40

2.1 Enterprise Cloud Customer Portal 40

2.1.1 Available Features 42

2.1.2 List of Items That Can Be Controlled 44

2.1.3 Important Points 45

2.2 Security Web Portal 46

2.2.1 Available Features 48

2.2.2 Important Points 50

3. Compute (Global Standard Menu) 51

3.1 Compute Resource 51

3.1.1 Available Features 51

3.1.2 Provision of Compute Resource Pools 52

3.1.3 Features for Controlling Compute Resource Pools 56

3.1.4 vApp Feature 57

3.1.5 Assigning Resources to a Virtual Machine 57

3.1.6 Important Points 69

3.2 Compute Resource (Dedicated Device) 74

3.2.1 Available Features 74
3.2.2 Provision of Compute Resource Pools....75
3.2.3 Parameter Settings for Resources....82
3.2.4 Assigning Resources to a Virtual Machine 83
3.2.5 Important Points 85
3.3 Private Catalog....87
3.3.1 Available Features 87
3.3.2 Provision of a Disk for Saving Template Catalogs....88
3.3.3 Create Template Feature....88
3.3.4 Import Template Feature 89
3.3.5 Export Template Feature....91
3.3.6 Important Points 91
3.4 OS License 92
3.4.1 Available Features 92
3.4.2 Provision of an OS License....92
3.4.3 Provision of a Public Catalog 93
3.4.4 Important Points 93
3.5 Database License (MS SQL) 96
3.5.1 Available Features 96
3.5.2 Provision of a Database License 96
Provision of a Public Catalog 96
3.5.3 Important Points 97
3.5.4 Initial State of Microsoft SQL Server 99
3.6 Microsoft SAL (RDS SAL) 111
3.6.1 Available Features 111
3.6.2 Provision of an RDS SAL....112
3.6.3 Provision of a Public Catalog 112
3.6.4 Important Points 113
4. Backup (Global Standard Menu) 114
4.1 Image Backup....114
4.1.1 Available Features....114
4.1.2 Backup and Restore....114
4.1.3 Backup and Restore Management 116
4.1.4 Important Points....118
4.2 File Backup....122

4.2.1 Available Features 122
4.2.2 Backup File Storage 123
4.2.3 Backup File Restore 124
4.2.4 Backup and Restore Management 124
4.2.5 Important Points 126

5. Network Features (Global Standard Menu) 130
5.1 Internet Connectivity 130
5.1.1 Available Features 130
5.1.2 An Internet GW Is Provided 130
5.1.3 Global IP Addresses Are Provided 131
5.1.4 Important Points 133
5.2 VPN Connectivity 134
5.2.1 Available Features 134
5.2.2 VPN Gateway 134
5.2.3 VPN Routing Settings 135
5.2.4 Enterprise Cloud and VPN Routing Design 135
5.2.5 Important Points 136
5.3 Server Segment 139
5.3.1 Available Features 139
5.3.2 Server Segments Are Provided 139
5.3.3 Important Points 143
5.4 Service Interconnectivity 144
5.4.1 Available Features 144
5.4.2 Service Interconnect Gateway 146
5.4.3 Routing Settings 146
5.4.4 Important Points 146
5.5 Colocation Interconnectivity 148
5.5.1 Available Features 148
5.5.2 Layer 2 (L2) Connection 148
5.5.3 Important Points 151
5.6 On-Premises Interonnectivity 152
5.6.1 Available Features 152
5.6.2 Layer 2 (L2) Connection 152
5.6.3 Important Points 157
5.7 vFirewall 158

5.7.1 Available Features 159
5.7.2 Routing Feature 160
5.7.3 Firewall Feature 160
5.7.4 Packet Filtering Feature 162
5.7.5 NAT/NAPT Feature 163
5.7.6 Important Points 163
5.8 vLoad Balancer 164
5.8.1 Available Features 165
5.8.2 Load Balancing Feature 165
5.8.3 Routing Feature 168
5.8.4 IP Address Delivery Feature 168
5.8.5 Important Points 170
5.9 Integrated Network Appliance 171
5.9.1 Available Features 171
5.9.2 Firewall Feature 174
5.9.3 NAT/NAPT Feature 175
5.9.4 Routing Feature 177
5.9.5 Load Balancing Feature 178
5.9.6 IPsec Termination Function 179
5.9.7 Important Points 182
5.9.8 Reference Information 184

6. External Storage (Global Standard Menu) 185
6.1 Global File Storage (Global Data Backup) 185
6.1.1 Available Features 186
6.1.2 Provides Storage for Saving Data 186
6.1.3 Data Replication Feature (Burst Feature) 188
6.1.4 Important Points 190

7. Security Features (Global Standard Menu) 192
7.1 IPS/IDS 192
7.1.1 Available Features 192
7.1.2 IPS/IDS Feature 192
7.1.3 Important Points 194
7.2 Email-Anti-Virus 196
7.2.1 Available Features 196
7.2.2 Virus Scan Feature 196

7.2.3 Important Points 198
7.3 Web-Anti-Virus 200
7.3.1 Available Features 200
7.3.2 Virus Scan Feature 200
7.3.3 Important Points 202
7.4 URL Filtering 204
7.4.1 Available Features 204
7.4.2 URL Filtering Feature 204
7.4.3 Important Points 206
7.5 Application Filtering 208
7.5.1 Available Features 208
7.5.2 Application Filtering Feature 208
7.5.3 Important Points 210
7.6 Web Application Firewall (WAF) 212
7.6.1 Available Features 212
7.6.2 Web Application Firewall Feature 212
7.6.3 Important Points 215
7.7 VM Anti-Virus 216
7.7.1 Available Features 216
7.7.2 Real Time Scan Feature 216
7.7.3 Scheduled Scan Feature 217
7.7.4 Actions 217
7.7.5 Scan Exception Feature 219
7.7.6 Pattern File Automatic Update Feature 219
7.7.7 Important Points 219
7.8 VM Virtual Patch 222
7.8.1 Available Features 222
7.8.2 VM Virtual Patch Feature 222
7.8.3 Recommended Scan Feature 223
7.8.4 Important Points 223
7.9 VM Firewall 226
7.9.1 Available Features 226
7.9.2 VM Firewall 226
7.9.3 Important Points 227
7.10 Application Profiling 230
7.10.1 Available Features 230

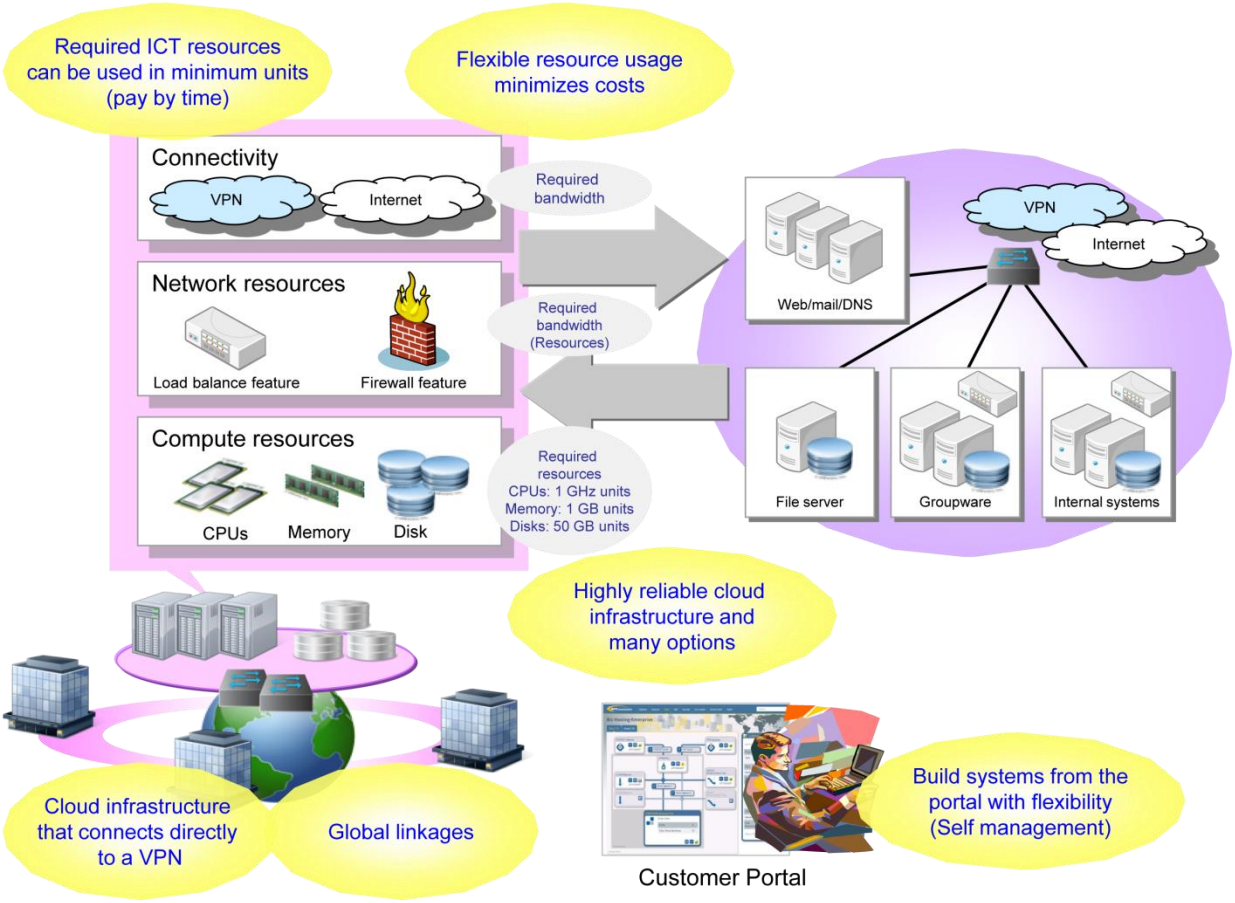
7.10.2 Application Profiling Report 230
7.10.3 Important Points 232
7.11 Network Profiling 233
7.11.1 Available Features 233
7.11.2 Network Profiling Report 233
7.11.3 Important Points 235
7.12 RTMD Web 236
7.12.1 Available Features 236
7.12.2 File Analysis Feature 236
7.12.3 Traffic Analysis Feature 237
7.12.4 Report Feature 237
7.12.5 Important Points 238
7.13 RTMD Email 238
7.13.1 Available Features 239
7.13.2 File Analysis Feature 239
7.13.3 Important Points 241
8. Maintenance and Operation of the Enterprise Cloud (Japan Contract) 242
8.1 Set of Materials Sent When You Start Using the Service 242
8.2 Customer Support 243
8.2.1 Support Center/Technical Help Desk 243
8.2.2 Maintenance and Operations System 244
8.3 Contact When a Failure Occurs 245
8.3.1 Items Monitored Remotely and Procedures for Notifying Users 246
8.3.2 Remote Monitoring System 247
8.4 Maintenance Information 249
8.5 Limitations to Maintenance Operations 250
Index 251
[Revision History] 253

1.Overview of the Enterprise Cloud

1.1 What is Enterprise Cloud?

The Enterprise Cloud uses the cloud infrastructure at the NTT Communications robust Data Centers to provide ICT resources, such as Compute Resources, firewalls, load balancers, Internet Connectivity, and VPN Connectivity.

The characteristics of Enterprise Cloud are described below.



Platform

In addition to server virtualization technology, network virtualization technology is also used within Data Centers and for networks between Data Centers, allowing flexibility when providing resources, and a high degree of self-management.

You can also specify and use cloud infrastructure from Data Centers located in Japan, America, Europe, Singapore, and Hong Kong.

Customer Portal

From the Customer Portal, you can add and delete Virtual Machines, edit the settings policy for vFirewall and vLoad Balancer, and increase or decrease each resource in real time.

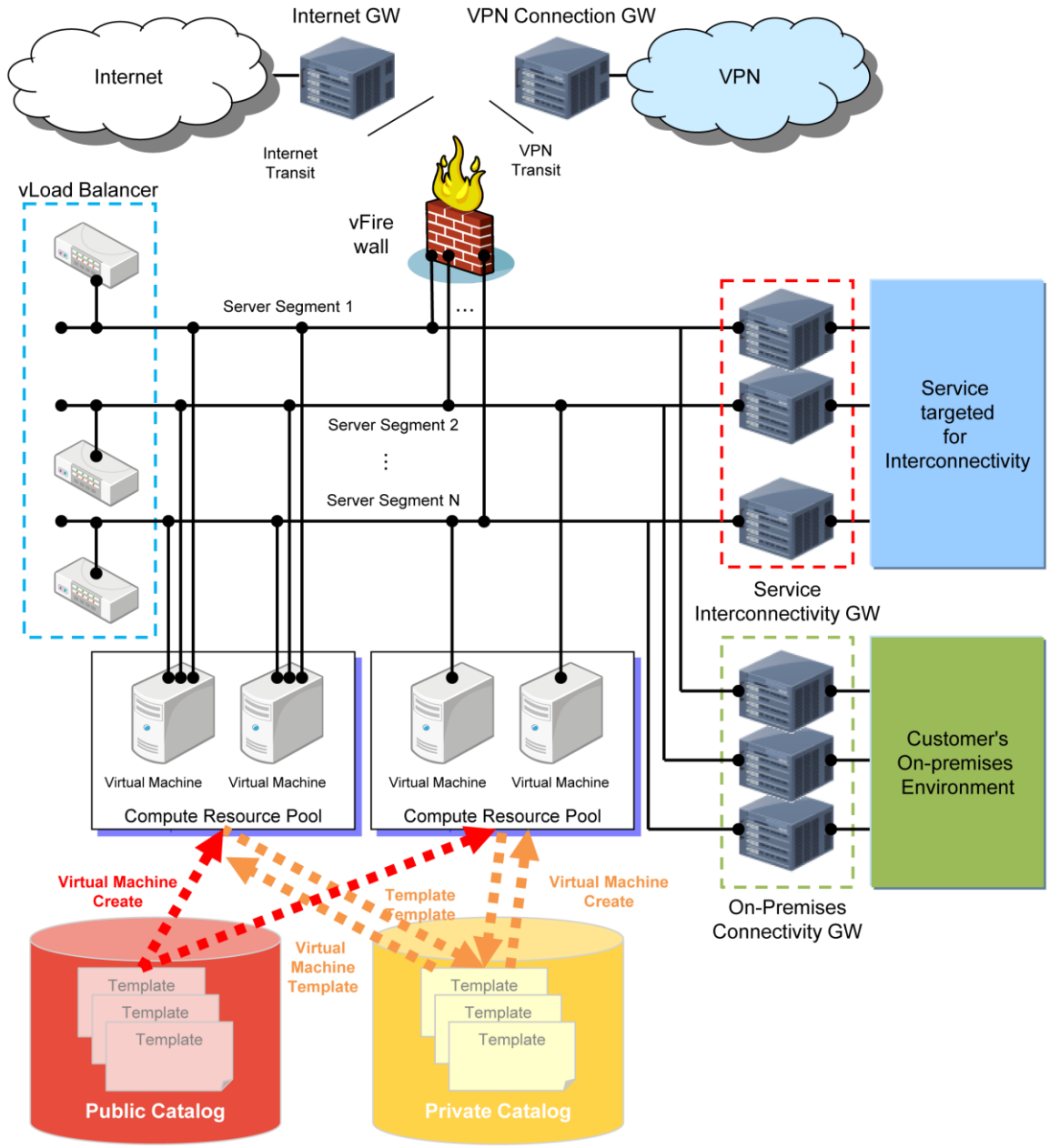
You can control all Data Center resources through one user interface.

1.2 Features that make up Enterprise Cloud

The available menus can be grouped into the following two main categories.

Menu	Overview
Global Standard Menu	This is a standard menu that is available for all Data Centers in the Enterprise Cloud. ※ For information on availability at each Data Center, refer to "1.3.2 Available Data Centers" (⇒P.21).
Local Option Menu	Options menus provided by each individual Data Center. Connects through the Service Interconnect Gateway. ※ For details regarding the local option menus, refer to the separate documentation.

The configuration of the Enterprise Cloud is shown below.



To use each feature included in the service, you need to apply for the services shown in the table below.

Component	Overview	Name of Service for Which You Need to Apply
Internet GW	Gateway for connecting to the Internet	Internet Connectivity (Global IP Address)
Internet Transit	Connects the Internet GW and the vFirewall ● A Global IP Address is provided.	
VPN Gateway	Gateway for connecting to a VPN	VPN Connectivity
VPN Transit	Connects the VPN Gateway and the vFirewall	
Firewall	A feature that provides a firewall between the Internet Transit, the VPN Transit, and the Server Segment.	vFirewall/Integrated Network Appliance
Load Balancer	A virtual dedicated load balancer on the Server Segment	vLoad Balancer/Integrated Network Appliance
Server Segment	An L2 segment feature for connecting the following devices ● Virtual Machine ● vFirewall ● vLoad Balancer ● Service Interconnect Gateway	Server Segment
Virtual Machine	Virtual dedicated server ● Resources are assigned and created from a Compute Resource Pool.	Compute Resource Compute Resource (Dedicated Device)
Compute Resource Pool	Resources for creating a Virtual Machine (CPU/Memory/Disk)	
Template	A Virtual Machine image, created by taking a copy of the server ● You can create a Virtual Machine using a template.	
Public Catalog	An area for storing registered templates that can be used by anyone	
Private Catalog	An area for storing templates that are exclusively for you	Private Catalog
Service Interconnect Gateway	A gateway for connecting Server Segments and other services provided by NTT Communications	Service Interconnectivity

Global File Storage (Global Data Backup)	A feature for backing up the desired data to a remote (Japan or overseas) Data Center ● Provided through the Service Interconnect Gateway.	Global File Storage (Global Data Backup)
On-Premises GW	A gateway that provides an L2 connection to Server Segments in your system environment (called the "On-Premises Environment" below) within your own operating system environment.	On-Premises Interconnectivity
Colocation Interconnectivity	Provides a secure L2 connection between the Server segment and Customer Colocation	Colocation Interconnectivity
Other Service Environment	Unique services offered by each Data Center ● They can be used in conjunction with Enterprise Cloud.	Local Option Menu

1.3 Services Available at All Data Centers (Global Standard Menu)

In Enterprise Cloud, you can use the following menus at all Data Centers.

Category	Service Name			Overview	Reference
Compute	Compute Resource		Compute Class	Provides the CPUs and Memory for creating a Virtual Machine by virtualizing a physical server shared by multiple users.	⇒P.51
			Storage Class	Provides the Disks for creating a Virtual Machine by virtualizing storage devices shared by multiple users.	⇒P.51
	Compute Resource (Dedicated Device)		Compute Class	Provides the CPUs and Memory for creating a Virtual Machine by virtualizing a physical server dedicated to you.	⇒P.74
			Storage Class	Provides the Disks for creating a Virtual Machine by virtualizing a storage device dedicated to you.	⇒P.74
	Private Catalog			Provides a Disk for storing templates of the Virtual Machines that you create. You can quickly create new Virtual Machines from the saved templates.	⇒P.87
	License	OS	Windows Server	Provides a Microsoft Windows Server license for Virtual Machines.	⇒P.92
			Red Hat Enterprise Linux	Provides a Red Hat Enterprise Linux subscription for Virtual Machines.	⇒P.92
		Database		Provides a Microsoft SQL Server license for Virtual Machines.	⇒P.96
		Microsoft SAL	RDS SAL	Provides a Microsoft Remote Desktop Service Subscriber Access License.	⇒P.111
	Image Backup			Provides a feature for backing up the current state of an entire Virtual Machine.	⇒P.114

	File Backup	Provides a feature for backing up files and folder in Virtual Machine.	⇒P.110

Networking	Internet Connectivity		Provides redundant Internet Connectivity. A Global IP Address is not normally included in "Internet Connectivity."	⇒P.130
	VPN Connectivity		Provides a connection with the Arcstar Universal One Service (NTT Communications' VPN service).	⇒P.134
	Server Segment		Provides an L2 segment that extends the Server Segment and interconnects the services that make up a Virtual Machine.	⇒P.139
	Inter-connectivity	Service Inter-connectivity	Provides Service Interconnect Gateways when using interconnectivity services such as global file storage (Global Data Backups) and other options.	⇒P.144
		Colocation Inter-connectivity	Provides a feature for having a secure L2 connection between the Server Segments in Enterprise Cloud and your system environment within NTT Communications Colocation.	⇒P.148
		On-Premises Inter-connectivity	Provides a feature for having a secure L2 connection between Server Segments in the Enterprise Cloud and an On-Premises Environment, through the Internet.	⇒P.152
	vFirewall		The main firewall features that are provided are a routing feature, packet filtering feature, and NAT/NAPT feature.	⇒P.158
	vLoad Balancer		Provides a virtual load balancer device on a Server Segment. You can use the load balancing feature for communication with Virtual Machines in a Server Segment.	⇒P.164
	Integrated Network Appliance		Provides Firewall, NAT/NAPT, Routing, Load Balancing, and IPSec termination function	⇒P.171
External Storage	Global File Storage (Global Data Backup)		Provides a feature for storing desired data in a remote (Japan or overseas) Data Center.	⇒P.185

Security	IPS/IDS	Provides a feature for detecting and blocking unauthorized access and cyber-attacks on a Virtual Machine.	⇒P.192
	Email-Anti-Virus	Provides a feature for inspecting for viruses in SMTP communication, such as files attached to emails, and detecting and blocking viruses.	⇒P.196
	Web-Anti-Virus	Provides a feature for inspecting for viruses in HTTP communication, such as website downloads, and detecting and blocking viruses.	⇒P.200
	URL Filtering	Provides a feature for controlling access to websites (warning/blocking).	⇒P.204
	Application Filtering	Provides a feature for blocking communication with specific applications.	⇒P.208
	WAF (Web Application Firewall)	Provides a feature for blocking unauthorized access and cyber-attacks on web applications.	⇒P.212
	VM Anti-Virus	Provides a feature for detecting and destroying viruses on a Virtual Machine.	⇒P.216
	VM Virtual Patch	Provides a feature for blocking attacks aimed at vulnerable OSs, middleware, and applications on a Virtual Machine.	⇒P.222
	VM Firewall	Provides a feature for controlling communication between Virtual Machines.	⇒P.226
	Application Profiling	Provides monitoring of application communication and advisory reports from a security profiler.	⇒P.230
	Network Profiling	Provides monitoring of unauthorized access and viruses, and advisory reports from a security analyst.	⇒P.233
	RTMD Web	Provides a feature for analyzing files downloaded from websites, and detecting and	⇒P.236

			reporting unknown malware.	
	RTMD Email		Provides a feature for analyzing files attached to emails, and detecting and reporting unknown malware.	⇒P.238
	Packaged Menu	Unauthorized Access Prevention	Consists of "IPS/IDS" and "Web-Anti-Virus". Features comply with those of the original menus.	-
		Web Browsing Security	Consists of "Web-Anti-Virus" and "URL Filtering". Features comply with those of the original menus.	-
		Internet Gateway Security	Consists of "IPS/IDS", "Web-Anti-Virus" and "URL Filtering". Features comply with those of the original menus.	-
		VM Security Advanced Package	Consists of "VM Anti-virus", "VM Virtual Patch" and "VM Firewall". Features comply with those of the original menus.	-

INFO
- Product availability depends on the Data Center. For details, refer to "1.3.2 Available Data Centers" (⇒P.21).

1.3.1 Available Equipment Environment

The equipment environment and performance guarantee for each menu are shown below.

For shared equipment, your contracted environment is logically independent by using server virtualization technology and VLAN technology.

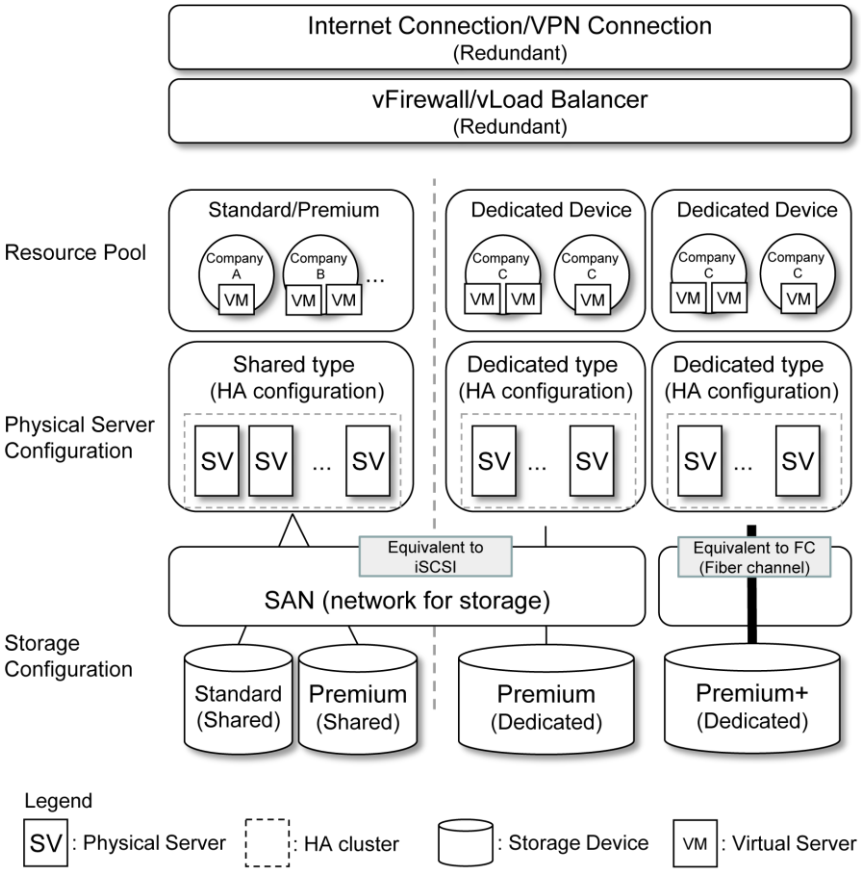
Service Name			Physical Equipment Environment	Performance Guarantee
Compute Resource	Compute Class	Guaranteed	Shared	Contracted value for CPU/Memory resources: Guaranteed
		Premium	Shared	Contracted value for CPU/Memory resources: Guaranteed
		Standard	Shared	Contracted value for

				CPU/Memory resources: Best Effort
	Storage Class	Premium	Shared	Contracted value for Disk resources: Guaranteed
		Standard	Shared	Contracted value for Disk resources: Guaranteed
Compute Resource (Dedicated Device)			Dedicated	Resources that provide dedicated devices: Guaranteed ※ Any value can be set for the CPU/Memory/Disk resources
Private Catalog			Shared	Contracted value for Disk resources: Guaranteed
License	OS	Windows Server	-	-
		Red Hat Enterprise Linux	-	-
	Database	MS-SQL	-	-
	Microsoft SAL	RDS SAL	-	-
Internet Connectivity	Best Effort		Shared	Contracted bandwidth: Best Effort
	Guaranteed		Shared	Contracted bandwidth: Guaranteed
	Global IP Address		-	-
VPN Connectivity	Best Effort		Shared	Contracted bandwidth: Best Effort
	Guaranteed		Shared	Contracted bandwidth: Guaranteed
Server Segment			Shared	Bandwidth for traffic usage: Best Effort
Interconnectivity	Service Inter-connectivity		Shared	Bandwidth for traffic usage: Best Effort
	Colocation Inter-connectivity		Shared	Bandwidth for traffic usage: Best Effort
	On-Premises Inter-		Devices in the Data	Contracted bandwidth: Best Effort

	connectivity	Center: Shared Devices in the On-Premises Environment : Dedicated	
vFirewall		Shared	Resource processing capacity: Maximum value guaranteed
vLoad Balancer		Shared	Resource processing capacity: Maximum value guaranteed
Integrated Network Appliance		Shared	Resource processing capacity: Best Effort.
Global File Storage (Global Data Backup)		Shared	Contracted Disk capacity: Guaranteed Bandwidth usage: Best Effort
IPS/IDS		Shared	Amount of traffic: Best Effort
Email-Anti-Virus		Shared	Amount of traffic: Best Effort
Web-Anti-Virus		Shared	Amount of traffic: Best Effort
URL Filtering		Shared	Amount of traffic: Best Effort
Application Filtering		Shared	Amount of traffic: Best Effort
Web Application Firewall (WAF)		Dedicated	Amount of traffic: Best Effort
VM Anti-Virus		-	-
VM Virtual Patch		-	-
VM Firewall		-	-
Application Profiling		Shared	Amount of traffic: Best Effort
Network Profiling		Shared	Amount of traffic: Best Effort
RTMD Web		Dedicated	Amount of traffic: Best Effort
RTMD Email		Dedicated	Amount of traffic: Best Effort

A diagram of the accommodated customers for Compute Resources is shown below.

INFO
- The diagram below is a logical configuration diagram. It is not an accurate representation of the actual physical configuration.


Internet Connection/VPN Connection
(Redundant)
vFirewall/vLoad Balancer
(Redundant)
Resource Pool
Standard/Premium
Company A
Company B
VM
Dedicated Device
Company C
Physical Server Configuration
Shared type
(HA configuration)
Dedicated type
(HA configuration)
SV
Equivalent to iSCSI
Equivalent to FC (Fiber channel)
SAN (network for storage)
Storage Configuration
Standard (Shared)
Premium (Shared)
Premium (Dedicated)
Premium+ (Dedicated)
Legend
: Physical Server
: HA cluster
: Storage Device
: Virtual Server

1.3.2 Available Data Centers

The Enterprise Cloud Data Centers are shown below.

Country	Abbreviation	Name
Japan	JP	Yokohama No.1 Data Center Kansai1 Data Center Saitama No.1 Data Center
USA	US	San Jose Lundy Data Center Virginia Sterling Data Center
UK	UK	Hemel Hempstead2 Data Center
Singapore	SG	Singapore Serangoon Data Center
Hong Kong	HK	Hong Kong Tai Po Data Center
Malaysia	MY	Malaysia Cyberjaya3 Data Center
Thailand	TH	Thailand Bangna Data Center
Australia	AU	Australia Sydney1 Data Center
Germany	DE	Germany Frankfurt2 Data Center

Services Provided by Each Data Center

The services that can be used at each Data Center are shown below.

Name of Menu/Feature			JP			US		UK
			Yokohama	Kansai1	Saitama	Lundy	Sterling	
Compute Resource	Compute Class	Guaranteed	Y	Y	Y	Y	Y	Y
		Premium	Y	Y	N	Y	Y	Y
		Standard	Y	Y	N	Y	Y	Y
	Storage Class	Premium	Y	Y	Y	Y	Y	Y
		Standard	Y	Y	Y	Y	Y	Y
	Zone*1		Y	Y	Y	N	N	N
Compute Resource (Dedicated Device)	Compute Class	Small	Y	Y	Y	N	N	N
		Medium	N	N	N	N	N	N
		Large	Y	Y	Y	N	N	N
	Storage Class	Premium	Y	Y	Y	N	N	N
		Premium+	Y	Y	Y	N	N	N
Private Catalog			Y	Y	Y	Y	Y	Y
License	OS	Windows Server	Y	Y	Y	Y	Y	Y
		Red Hat Enterprise Linux	Y	Y	Y	Y	Y	Y
	Database	MS SQL	Y	Y	Y	Y	Y	Y
	Microsoft SAL	RDS SAL	Y	Y	Y	Y	Y	Y
Image Backup			Y	Y*5	Y	N	Y	N
File Backup			Y	N	Y	N	N	N
Internet Connectivity	Best Effort	10 Mbps	Y	Y	Y	Y	Y	Y
		100 Mbps	Y	Y	Y	Y	Y	Y
		1 Gbps	Y	Y	Y	Y	Y	Y
	Guaranteed	1 to 100 Mbps	Y	Y	Y*2	Y*2	Y*2	Y*2
		200 Mbps to 1 Gbps	Y	Y	Y	Y	Y	Y
	Global IP Address		Y	Y	Y	Y	Y	Y
VPN Connection	Best Effort	100 Mbps	Y	Y	Y	Y	Y	Y
	Guaranteed	100 Mbps	Y	Y	Y	N	N	N
		200 Mbps	Y	Y	Y	N	N	N
		1 Gbps	Y*6	Y	Y*6	N	N	N
Server Segment			Y	Y	Y	Y	Y	Y
Interconnectivity	Service Interconnectivity		Y	Y	Y	Y	Y	Y
	Collocation Interconnectivity		Y	Y	Y	N	N	N
	On-Premises Connectivity		Y	N	N	N	N	N
vFirewall			Y	Y	Y	Y	Y	Y
vLoad Balancer			Y	Y	Y	Y	Y	Y
Integrated Network Appliance			Y	Y	Y	Y	Y	Y
Global File Storage (Global Data Backup)	Local Storage		Y	Y	Y	Y	Y	Y
	Remote Storage (Domestic)		Y	Y	Y	Y	Y	N
	Remote Storage (Global)		Y	Y	Y	Y	Y	Y
IPS/IDS			Y	Y	N	Y	Y	Y
Email-Anti-Virus			Y	Y	N	Y	Y	Y
Web-Anti-Virus			Y	Y	N	Y	Y	Y
URL Filtering			Y	Y	N	Y	Y	Y
Application Filtering			Y	Y	N	Y	Y	Y
Unauthorized Access Prevention			Y	Y	N	Y	Y	Y
Web Browsing Security			Y	Y	N	Y	Y	Y

Internet Gateway Security	Y	Y	N	Y	Y	Y
Web Application Firewall (WAF)	Y*3	Y*3	N	Y*3	Y*3	Y*3
VM Anti-Virus	Y	Y	Y	Y	Y	Y
VM Virtual Patch	Y	Y	Y	Y	Y	Y
VM Firewall	Y	Y	Y	Y	Y	Y
VM Security Advanced Package	Y	Y	Y	Y	Y	Y
Application Profiling	Y*4	Y*4	N	Y*4	Y*4	Y*4
Network Profiling	Y*4	Y*4	N	Y*4	Y*4	Y*4
RTMD Web	Y*4	Y*4	Y*4	Y*4	Y*4	Y:4
RTMD Email	Y*4	Y*4	Y*4	Y*4	Y*4	Y*4

Name of Menu/Feature			DE	SG	HK	MY	AU	TH
Compute Resource	Compute Class	Guaranteed	Y	Y	Y	N	Y	Y
		Premium	N	Y	Y	Y	Y	Y
		Standard	N	Y	N	N	N	N
	Storage Class	Premium	Y	Y	Y	Y	Y	Y
		Standard	Y	Y	N	N	N	N
	Zone		N	N	N	N	N	N
Compute Resource (Dedicated Device)	Compute Class	Small	N	N	N	N	N	N
		Medium	N	N	N	N	N	N
		Large	N	N	N	N	N	N
	Storage Class	Premium	N	N	N	N	N	N
		Premium+	N	N	N	N	N	N
Private Catalog			Y	Y	Y	Y	Y	Y
License	OS	Windows Server	Y	Y	Y	Y	Y	Y
		Red Hat Enterprise Linux	Y	Y	Y	Y	Y	Y
	Database	MS SQL	Y	Y	Y	Y	Y	Y
	Microsoft SAL	RDS SAL	Y	Y	Y	Y	Y	Y
Image Backup			N	N	N	N	N	N
File Backup			N	N	N	N	N	N
Internet Connectivity	Best Effort	10 Mbps	Y	Y	N	Y	Y	Y
		100 Mbps	Y	Y	Y	Y	Y	Y
		1 Gbps	N	N	N	N	N	N
	Guaranteed	1 to 100 Mbps	Y*2	Y*2	N	Y*2	Y*2	Y*2
		200 Mbps to 1 Gbps	N	Y	N	N	N	N
	Global IP Address		Y	Y	Y	Y	Y	Y
VPN Connection	Best Effort	100 Mbps	Y	Y	Y	Y	Y	Y
	Guaranteed	100 Mbps	N	N	N	N	N	N
		200 Mbps	N	N	N	N	N	N
		1 Gbps	N	N	N	N	N	N
Server Segment			Y	Y	Y	Y	Y	Y
Interconnectivity	Service Interconnectivity		Y	Y	Y	Y	Y	Y
	Collocation Interconnectivity		N	N	N	N	N	N
	On-Premises Connectivity		N	N	N	N	N	N
vFirewall			N	Y	Y	Y	Y	Y
vLoad Balancer			N	Y	Y	Y	Y	Y
Integrated Network Appliance			Y	N	N	N	N	N
Global File Storage (Global Data	Local Storage		Y	Y	Y	Y	Y	Y
	Remote Storage (Domestic)		N	N	N	N	N	N

Backup)	Remote Storage (Global)	N	Y	Y	Y	Y	N
IPS/IDS		Y	Y	Y	Y	Y	Y
Email-Anti-Virus		Y	Y	Y	Y	Y	Y
Web-Anti-Virus		Y	Y	Y	Y	Y	Y
URL Filtering		Y	Y	Y	Y	Y	Y
Application Filtering		Y	Y	Y	Y	Y	Y
Unauthorized Access Prevention		Y	N	N	N	N	N
Web Browsing Security		Y	N	N	N	N	N
Internet Gateway Security		Y	N	N	N	N	N
Web Application Firewall (WAF)		Y*3	Y*3	Y*3	Y*3	Y*3	Y*3
VM Anti-Virus		Y	Y	Y	Y	Y	Y
VM Virtual Patch		Y	Y	Y	Y	Y	Y
VM Firewall		Y	Y	Y	Y	Y	Y
VM Security Advanced Package		Y	Y	Y	Y	Y	Y
Application Profiling		Y*4	Y*4	Y*4	Y*4	Y*4	Y*4
Network Profiling		Y*4	Y*4	Y*4	Y*4	Y*4	Y*5
RTMD Web		Y*4	Y*4	Y*4	Y*4	Y*4	Y*4
RTMD Email		Y*4	Y*4	Y*4	Y*4	Y*4	Y*4

※Please contact directly for service description

※1 Zone function is provided for Guaranteed Compute/Premium Storage. Zone function in other Data Center is scheduled to be provided in the near future.

※2 10Mbps Guaranteed and 100Mbps Guaranteed are available.

※3 Device individually procured. Please inquire for service specification.

※4 Device procurement and/or network design and so on are individually required. Please inquire for service specification.

※5 Need to use Order form.

※6 1Gbps Gurantanteed is not be available in Customer Portal available VPN Connectivity Service.

1.3.3 Service Order, Delivery Time and Minimum Usage Period

Service Order

The service order for each service is shown below.

NOTE ● An application is required to use each Data Center.

Service Name		New	Changes	Addition/ Deletion	Termi-nation
Compute Resource	Compute Class	Application	Customer Portal	Customer Portal	Application
	Storage Class	Application	Customer Portal	Customer Portal	
Compute	Compute Class	Application	Application	Application	

Resource (Dedicated Device)	Storage Class		Application	-	Application (※1)
Private Catalog			Customer Portal	Customer Portal	Customer Portal
License	OS	Windows Server	Customer Portal	-	Customer Portal
		Red Hat Enterprise Linux	Customer Portal	-	Customer Portal
	Database	MS-SQL	Customer Portal	-	Customer Portal
	Microsoft SAL	RDS SAL	Customer Portal	-	Customer Portal
Image Backup			Customer Portal	Customer Portal	Customer Portal
File Backup			Application	Application	Application
Internet Connectivity(※5)			Customer Portal/ Application	Customer Portal/ Application (※2)	Customer Portal/ Application
VPN Connectivity(※6)			Application	Customer Portal/ Application	Application
Server Segment（※5）			Customer Portal/ Application	-	Customer Portal/ Application
Inter-connectivity	Service Interconnectivity		Application	Application	Application
	Colocation Interconnectivity		Application	Application	Application
	On-Premises Interconnectivity		Application	Application	Application
vFirewall			Application	Customer Portal	-
vLoad Balancer			Customer Portal	Customer Portal	Customer Portal
Integrated Network Appliance			Application	(※3)	-

Global File Storage (Global Data Backup)	Application	Application	Application	
Security	Application	Configuration Form /EC Customer portal(※4)	Application	Application

※1 The only possible change in the storage capacity is an increase.

※2 The Global IP Address can be added or deleted when using vFirewall. However, Global IP Address can not be added or deleted when using Integrated Network Appliance.

※3 Plan change can be done from Single to Redundant. However, plan change from Compact to Large is not possible.

※4 Configuration change requests are called PCRs (Policy Change Requests). The upper limit of the number of PCRs is 15 times per menu per year.

※5 Order in Customer Portal is available in Kansai1 and Saitama No.1 Data Center.

※6 Customer Portal for VPN Connectivity is available in Yokohama No.1 Data Center and Saitama No.1 Data Center.

Standard Delivery Time for Each Service which needs order form

The standard delivery times for each service which needs ordr form are shown below.

Service Name			New	Changes	Addition/ Deletion	Termi-nation (Service)
Compute Resource (※1)	Compute Class		5 business days	-	-	1 to 15 business days
	Storage Class		5 business days	-	-	
Compute Resource (Dedicated Device)			Please inquire	Please inquire	Please inquire	
Private Catalog			-	-	-	
License (※1)	OS	Windows Server	-	-	-	
		Red Hat Enterprise Linux	-	-	-	
	Database	MS-SQL	-	-	-	
	Microsoft SAL	RDS SAL	-	-	-	
Image Backup(※1)			-	-	-	
File Backup			Please inquire	Please inquire	Please inquire	
Internet Connectivity(※1) (※2)			-	-	-	
VPN Connectivity (※5)			17 business days (※3)	17 business days (※3, ※6)	17 business days (※3)	
VPN Connectivity(Customer Portal Availavle)			9 business days	(※1)	9 business days	
Server Segment(※1) (※2)			-	-	-	

Inter-connectivity	Service Interconnectivity	5 business days (※3)	5 business days (※3)	5 business days (※3)	
	Colocation Interconnectivity	18 business days (※3)	18 business days (※3)	18 business days (※3)	
	On-Premises Interconnectivity (※7)	17 business days (※3)	1 business day (※3)	1 business day (※3)	
vFirewall		5 business days	(※1)	-	
vLoad Balancer(※1)		-	-	-	
Integrated Network Appliance		5 business days	(※8)	-	
Global File Storage (Global Data Backup)		15 business days (※3)	15 business days (※3)	15 business days (※3)	
IPS/IDS		10 business days (※3)	10 business days (※3)	10 business days (※3)	10 business days
Email-Anti-Virus		10 business days (※3)	10 business days (※3)	10 business days (※3)	10 business days
Web-Anti-Virus		10 business days (※3)	10 business days (※3)	10 business days (※3)	10 business days
URL Filtering		10 business days (※3)	10 business days (※3)	10 business days (※3)	10 business days
Application Filtering		10 business days (※3)	10 business days (※3)	10 business days (※3)	10 business days
Web Application Firewall (WAF)		55 business days (※3)	10 business days (※3)	55 business days (※3)	10 business days
VM Anti-Virus (※9)		7 business days (※3)	7 business days (※3)	7 business days (※3)	5 business days
VM Virtual Patch (※9)		7 business days (※3)	7 business days (※3)	7 business days (※3)	5 business days
VM Firewall (※9)		7 business days (※3)	7 business days (※3)	7 business days (※3)	5 business days

Application Profiling	10 business days (※3)	-	10 business days (※3)	10 business days
Network Profiling	10 business days (※3)	-	10 business days (※3)	10 business days
RTMD Web	25 business days (※3)	5 business days (※3)	25 business days (※3)	10 business days
RTMD Email	25 business days (※3)	5 business days (※3)	25 business days (※3)	10 business days
Unauthorized Access Prevention	10 business days (※3)	10 business days (※3)	10 business days (※3)	10 business days
Web Browsing Security	10 business days (※3)	10 business days (※3)	10 business days (※3)	10 business days
Internet Gateway Security	10 business days (※3)	10 business days (※3)	10 business days (※3)	10 business days
VM Security Advanced Package (※9)	7 business days (※3)	7 business days (※3)	7 business days (※3)	5 business days

※1 Available to apply through the Customer Portal.

※2 5 business days is needed except for Kansai1 and Saitama No.1 Data Center. Because the funciton is not available in other Data Center.

※3 The standard delivery time for Japan Data Centers. Please check. The delivery times are different for each Data Center. Delivery times may vary depending on the status of NTT Communications' equipment.

※4 The number of Global IP Address cannot be changed in Integrated Network Appliance. Global IP Addess parameter cannot be changed in both vFirewall and Integrated Network Appliance.

※5 The guaranteed type requires individual adjustment.

※6 Customers who started using the VPN Connectivity at the Yokohama No.1 Data Center before November 15, 2013 and have not changed the bandwidth in the past will require loan work to change the bandwidth. Please be advised that you will be asked to specify the work days beyond the 17 business days.

※7 When replacing GW equipment on-premises due to failure, it will take 17 days.

※8 Plan change from Single to Redundant can be done from Customer Portal. Plan change between Compact and Large is not possible.

※9 This will not be applied if the Customer is using OS Management Service (Japan Local option).

Minimum Usage Period

The minimum usage period is one month from the time that you start using Enterprise Cloud.

However, minimum usage periods for the following service menus are specified separately.

Service Name	Minimum Usage Period
Compute Resource (Dedicated Device)	1 year

1.3.4 Resource Contract Conditions and Service Combination Conditions

Resource Contract Conditions

The following resource contracts are required for each Data Center.

Compute Resource/Compute Resource (Dedicated Device)	A contract for Compute Resource or Compute Resource (Dedicated Device) is required. The minimum resources when contracting Compute Resource are shown below. ● CPU: 1 GHz ● Memory: 1 GB ● Disk: 50 GB
Internet Connectivity/VPN Connectivity	Both contracts are available.
vFirewall/Integrated Network Appliance	A contract for either one of the menu is mandatory. Customer cannot have a contrat for both.

INFO

- Deleting all Compute Resources is not possible.
- You can only contract for one Internet Connectivity and one VPN Connectivity for each Data Center that you are using.

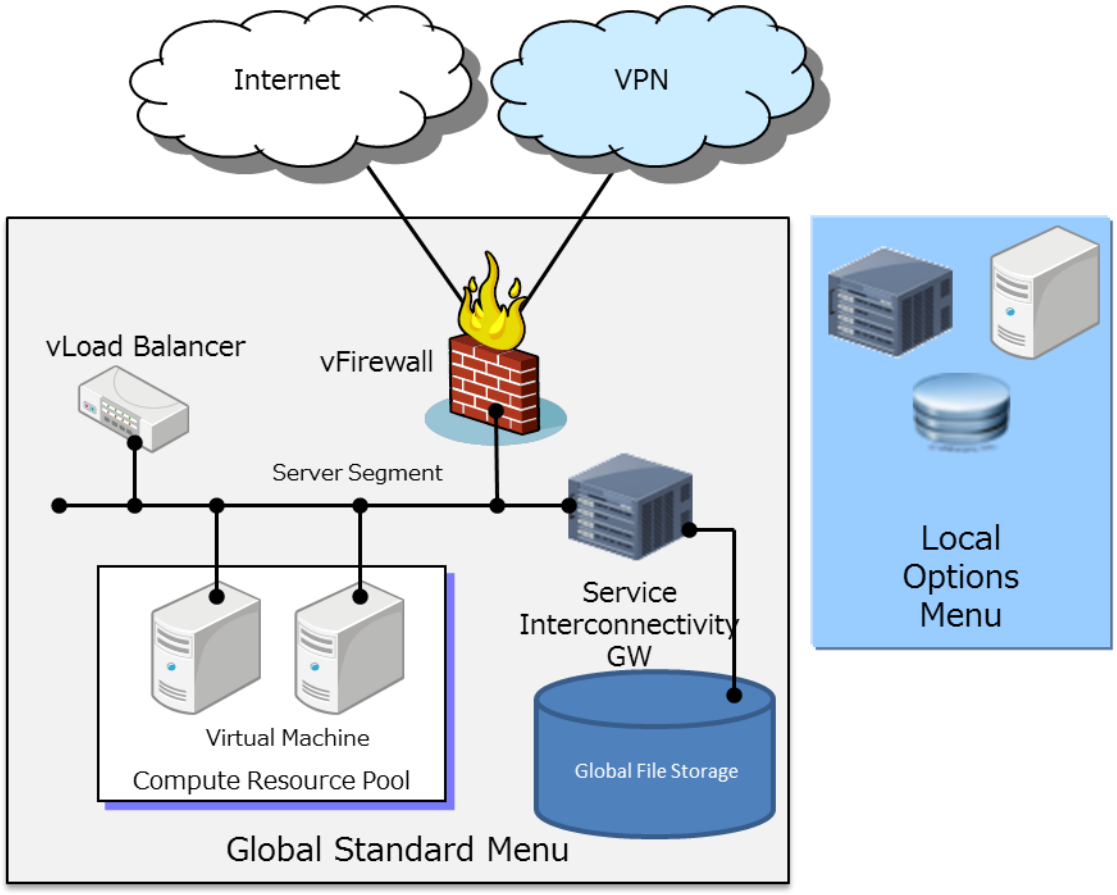
Combination Conditions

Global File Storage (Global Data Backup)	Can only be used through the Service Interconnect Gateway (※).
Database License	You cannot use Private Catalog and Image Backup on a Virtual Machine that uses a Database License (MS SQL) (when creating a Virtual Machine from a template stored in a Private Catalog, we cannot guarantee that it will work).
Colocation Interconnectivity On-Premises Interconnectivity	NTT Communications Server Segments are required for each customer system environment that is connecting.
Security	The following security services can only be used through Service Interconnect Gateway (※). ● IPS/IDS ● Email-Anti-Virus ● Web-Anti-Virus ● URL Filtering ● Application Filtering ● Web Application Firewall (WAF) ● Application Profiling ● Network Profiling

※ You need to apply separately for the Service.

1.4 Services That Have Data Center-Specific Usage (Local Option Menu)

The services available through the local option menu vary depending on which Data Center you are using.



NOTE

- You need to apply separately to use the local option menu. For details, please contact your NTT Communications sales representative.

INFO

- You can only use Global File Storage (Global Data Backup (Self)) through Service Interconnect Gateway.

The local option menu for Japan Data Centers is shown below.

Category	Service Name
OS License	Switch License
Database License	Oracle Database Standard Edition One
	Oracle Database Standard Edition RAC
	MS SQL SE for Cluster
License	HULFT
Authentication	Single Sign-On
External Storage	Block Storage
Networking	Remote Client Connection
System Management	OS Management
	IT Service Management
	Configuration Change/Maintenance Work Proxy
Hybrid	Hybrid Option MS Office365
	Hybrid Option Cloudn

1.5 Example Usage Model

This section provides examples of service combinations used for different usage applications.

When Used As a Test Environment/Development Environment

Required Features/Requests	Used Services and Notes
● I want the performance of the servers and networks to be Best Effort, and I want to keep the cost down as much as possible. ● I want to use a free OS. ● I want to prepare resources in the shortest time.	● Compute Resource: Use the Standard with the Compute Class (CPU/Memory) and storage class (Disk) ● Internet Connectivity: Use 10 Mbps Best Effort ● Private Catalog: Use Private Catalog to upload CentOS ● Can be prepared in the shortest time of 5 business days

When Building an In-house File Server

Required Features/Requests	Used Services and Notes
● I want to use it directly with the Arcstar Universal One service (the NTT Communications VPN service). ● I want to change the Disk write frequency and request speed by server.	● Internet Connectivity: Do not use ● VPN Connectivity: Use ● Compute Resource: Use the Compute Resource Pools separated by server (differentiate between the Compute Resource Pools that use the Standard and Premium Disk capacity)

When Building a New EC Site

Required Features/Requests	Used Services and Notes
● I want to precisely distribute the communication load to servers. ● I want to control resources in real time. ● I want to precisely guarantee the Internet bandwidth. ● I want to increase the performance of resources according to usage.	● vLoad Balancer: Use (distribute the server access load) ● Internet Connectivity: Use the guaranteed type ● Check the Customer Portal performance statistics report and add resources in real time

When Using the Cloud for Multiple Systems

Required Features/Requests	Used Services and Notes
● I want to separate network segments so that I can separate them into multiple systems. ● I want it to be easy to operate because I will be managing many servers.	● Server Segment: Add Server Segments and build a complex network ● Compute Resource: Separate and manage Compute Resource Pools by system

When Outsourcing an Application Server That Demands Performance for Data I/O

Required Features/Requests	Used Services and Notes
● I want to reliably secure Disk I/O. ● I cannot physically accommodate another contractor on the same server, so I want to use the cloud on a dedicated physical server.	● Compute Resource (Dedicated Device): The server equipment and storage devices in the cloud infrastructure are used by having a physical server in a physical enclosure dedicated to you

When Outsourcing an Infrastructure That Cannot Be Installed on the Same Hardware As Another Business, Due to the Security Policy

Required Features/Requests	Used Services and Notes
● I want to reliably secure Disk I/O. ● I cannot physically accommodate another contractor on the same server, so I want to use the cloud on a dedicated physical server.	● Compute Resource (Dedicated Device): The server equipment and storage devices in the cloud infrastructure are used by having a physical server in a physical enclosure dedicated to you

When Implementing a BCP

Required Features/Requests	Used Services and Notes
● I want my system to be in a robust Data Center rather than keeping the data within my company. ● I want to back up my data in another country.	● In Enterprise Cloud, the cloud infrastructure resides in robust Data Centers (characteristic of a carrier), regardless of which service you are using. ● Global File Storage (Global Data Backup): Important data is saved in a remote overseas location in real time

1.6 Explanation of Common Terms

This section explains common terms used in Enterprise Cloud.

Term	Definition
Compute Resource	A service that provides the virtual resources (CPU/Memory/Disk) to create Virtual Machines.
Compute Resource Pool (CRP)	A resource management unit (pool) created in Compute Resource
Compute Class	A name for distinguishing the performance of a CPU and Memory
Storage Class	A name for distinguishing the performance of a Disk
Compute Resource (Dedicated Device)	A service that provides virtual resources (CPU/Memory/Disk) using devices (physical server, storage devices) that are dedicated to the customer
Server Segment	A service that provides an L2 segment for connecting multiple services to each other in Enterprise Cloud
Firewall	A device for preventing penetration of Enterprise Cloud from the Internet
Load Balancer	A virtual dedicated load balancer for allocating requests to multiple servers
Service Interconnectivity	A service that provides interconnectivity between Enterprise Cloud and other services
VPN Connectivity	A service that provides VPN Connectivity through an application connection service for customers of the Arcstar Universal One service (NTT Communications' VPN service)
Gateway	A device required to communicate by connecting networks together
VPN Gateway	A device for connecting a VPN to Enterprise Cloud
VPN Transit	A device for connecting between VPN Gateway and vFirewall
Internet Connectivity	A service that provides Internet Connectivity for customers of Enterprise Cloud
Internet GW	A device for connecting the internet to Enterprise Cloud
Internet Transit	A device for connecting between the Internet GW and the vFirewall

Private Catalog	A service that provides an area where customers can store their own templates for creating Virtual Machines
Global File Storage (Global Data Backup)	A service that provides an External Storage area for storing backup data
On-Premises Environment	Your operational system environment at your company
On-Premises Interconnectivity	A service that provides a secure L2 connection between Server Segments in Enterprise Cloud and an On-Premises Environment, through the internet
Colocation	Installation of your system at a Data Center
Colocation Interconnectivity	A service that provides a secure L2 connection between the Server Segments in Enterprise Cloud and your system environment within NTT Communications Colocation, via our inter-Data Center network
On-Premises GW in a Data Center	A device for connecting between an NTT Communications Data Center and the Internet for On-premises Connectivity
On-Premises GW in Your On-Premises Environment	A device for connecting between your On-Premises Environment and the Internet, in order to establish On-premises Connectivity
IPS (Intrusion Prevention (Protection) System)	A system for preventing intrusions
IDS (Intrusion Detection System)	A system for detecting intrusions
Signature	A list in which known attack patterns and malware patterns are converted into data
Policy	Rules for detecting and interrupting communication
RPS (Requests Per Second)	The number of requests that are processed per second ※ The numerical value when the server makes one connection (when using One Connect on the server side) for multiple connections to a client.

CPS (Connections Per Second)	The number of connections that are processed per second ※ The numerical value when the server makes one connection for one connection to a client.
C&C Server (Command and Control Server)	The server that sends commands and becomes the center of control for a computer infected with malware
PCR	Policy Change Request
Active Device	A device that has priority of use
Standby Device	A device that is used when there is an error on the active device
vApp	A container for Virtual Machines managed by VMware.

1.7 Restrictions

- Customers cannot enter the hosting room in which the servers and other equipment provided by Enterprise Cloud are housed. All system construction work that you perform should be performed remotely.
- The common conditions for providing Enterprise Cloud, and service specifications and the conditions for providing each service may change without notice.
- When a contract or service is removed or canceled, or when you delete a service from the Customer Portal, the data will be erased according to the method specified by NTT Communications. A data erasure certificate is not issued.
- When you use Enterprise Cloud, you must comply with the laws of foreign countries and international trade and other Japanese import and export regulations, along with all applicable laws and regulations related to importing, reimporting, exporting, and reexporting to and from other countries and regions. In other words, you are solely responsible for compliance with laws and regulations related to all actions that are taken when using Enterprise Cloud, such as transferring, processing, and providing content.
- You may not use Enterprise Cloud for the development, production, or use of conventional weapons or weapons of mass destruction including nuclear weapons, as stipulated in the Foreign Exchange and Foreign Trade Law and other Japanese laws relating to exporting.

2.Service Management (Portal Site)

2.1 Enterprise Cloud Customer Portal

An Enterprise Cloud Customer Portal (called the "Customer Portal" below) is available to users for managing services. You can use the Customer Portal to create Virtual Machines and configure your network environment in real time.

Enterprise Cloud provides two types of Customer Portal.

Customer Portal ver1.0 and Customer Portal ver2.0 with new Graphic User Interface.

The availability of Customer Portal ver1.0 and 2.0 is listed below:

JP			US		UK	DE	SG	HK	MY	AU	TH
Yokohama	Kansai	Saitama	Lundy	Sterling							
1.0	1.0	2.0	1.0	1.0	2.0	2.0	1.0	1.0	1.0	1.0	1.0

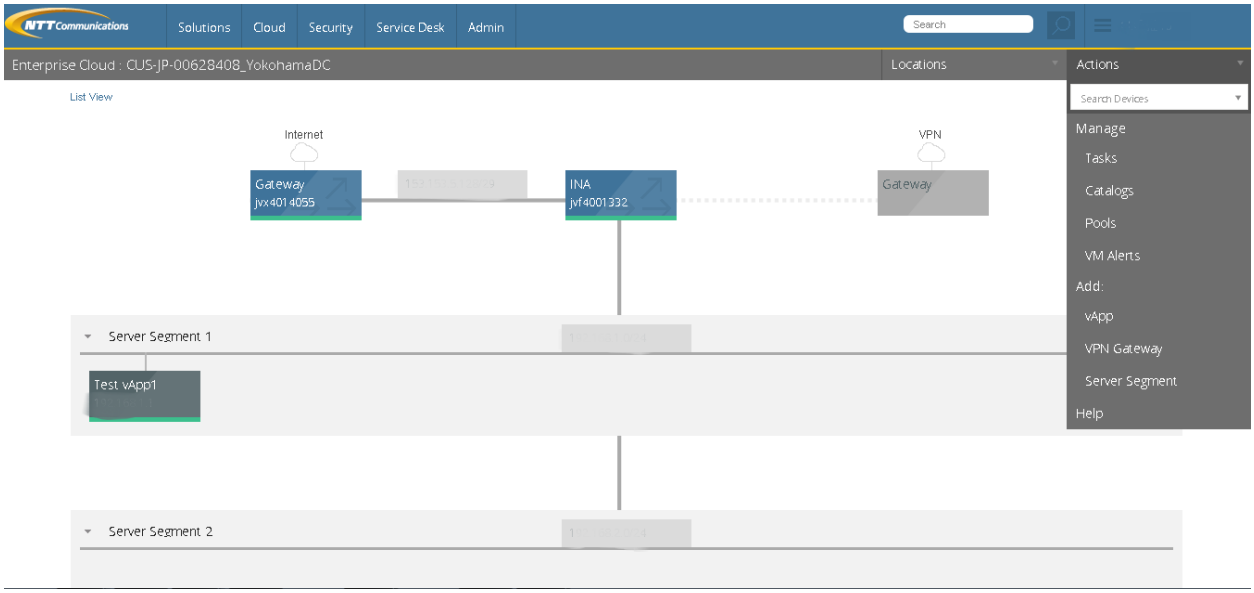
For some Enterprise Cloud services, Customer Portal ver2.0 provides different service specification from that of Customer Portal ver1.0 .

Customer Portal ver1.0	**All Service Specification is applied**
Customer Portal ver2.0	Following Services provide different service specification from Customer Portal ver1.0 . - Compute Resource (Please refer to) - MSSQL (Please refer to)

A diagram of the Enterprise Cloud Customer Portal ver1.0 usage is shown below.

NTT Communications
Solutions
Cloud
Service Desk
Admin
Enterprise Cloud
504490_KinrakujiDC
More Virtual Rooms
List View
Internet Gateway
jvx3900844
Internet Transit
VPN Transit
VPN Gateway
jvx3903283
Virtual Firewall
jvf3900538
Virtual Load Balancers
jvb3900563
Virtual Load Balancer
[1] - Server Segment 1
[2] - Server Segment 2
Server Segment
Gateways
Compute Resource Pools
Overview:
Pools 2
Total Virtual Machines 7

A diagram of the Enterprise Cloud Customer Portal ver2.0 usage is shown below.



INFO

- The Customer Portal is accessed using HTTPS communication through a web browser. Access to the Customer Portal requires authentication using the ID and password that you have been issued.

NTT Communications Business Portal

Enterprise Cloud is a service that is compatible with the NTT Communications Business Portal. You need to submit a separate application to use the service in conjunction with the Business Portal.

If you are using the service through the Business Portal, the authentication methods and user management procedures are different to those explained in this document. For details, refer to the "NTT Communications Business Portal User's Guide" available separately.

2.1.1 Available Features

You can use the following features in the Customer Portal.

Feature		Overview
Feature for batch management of multiple Data Centers.		You can manage multiple Data Centers as a batch.
Portal Feature	User Management	You can create and manage user accounts for accessing the Customer Portal.
	Ticket Feature※1	You can share information between you and NTT Communications, such as support assistance, communication regarding errors, and inquiries.
Control Feature	Virtual Resource Control	You can control the following resources. ● Add and delete Compute Resources

		(CPUs/Memory/etc.) ● Build, change, and delete Virtual Machines ● Monitor and graphically display Compute Resources and Virtual Machines ● Change the resources and set policies for firewalls and load balancers ● Add and change and terminate Internet Conncecitivity. ※2 ● Add and delete Server Segment※2. ● Change VPN Connectivity. ※2
	Console Connectivity	You can perform a console connection with a Virtual Machine using a web browser.
	Backup control	You can control the data synchronization process (boost process) between the primary storage and backup storage between Data Centers.

※1 In Case of using remote Data Centers without local Data Center, Customer Portal Ticket cannot be available. Please refer to 9.2.1 Support Center/Technical Help Desk.

※2 Available in Customer Portal function activated Data Center.

INFO
- Access to the Customer Portal requires authentication using an ID and password.

2.1.2 List of Items That Can Be Controlled

You can use the following operations in the Customer Portal.

Name of Menu/Feature			Create/ Execute	Display	Change	Delete
Compute Resource Pool	Compute Resource	CPU		Y	Y	
		Memory		Y	Y	
		Storage		Y	Y	
	Resource Pool		Y	Y	Y	Y
	Monitoring			Y		
Public Catalog	Virtual Machine Template/ vApp Template			Y		
Private Catalog	Resource (Storage Capacity)		Y	Y	Y	Y
	Template		Y	Y		Y
	Download Template		Y			
Take a Virtual Machine Template (OVA File)	Upload		Y			
Virtual Machine/vApp※4	Create a Virtual Machine/vApp	Private Catalog	Y			
		Use a Template				
		Public Catalog	Y			
		Use a Template				
	Resource	vCPU		Y	Y	
		Memory		Y	Y	
		Number of Disks	Y	Y		Y
		Disk Capacity		Y	Extension	
	vNIC (Select the Layout Segment)		Y	Y		
	Powered On, Powered Off, Reset, Shutdown, Suspend, Restart		Y	Y		
	Console Connectivity		Y	Y		
	ISO Image Mount Feature		Y			
	Install/UpdateVMware Guest Tools		Y			
	Set Guest Customization Enabled		Y			
	Enable Windows OS SID Modification Feature		Y			
	Monitoring, Log			Y		
Image Backup			Y	Y	Y	Y
File Backup			Y※1	Y	Y	Y
Internet Connectivity※2			Y	Y	Y	Y
VPN Connectivity※3	Bandwidth			Y	Y	
	Ping		Y			
	Routing Information		Y	Y	Y	Y
Server Segment	Segment Management※2		Y	Y		Y
	IP Address Management		Y	Y	Y	
Interconnectivity	Service Interconnectivity			Y		
	Collocation Connectivity			Y	Link Speed	
vFirewall	vFirewall Installation (Required)					
	Network Configuration			Y		
	Resource Level			Y	Y	
	Address or Object/Group		Y	Y	Y	Y
	Service or Object/Group		Y	Y	Y	Y
	Filtering Rules		Y	Y	Y	Y
	NAT/NAPT		Y	Y	Y	Y
	GIP			Y		

	Routing	Y	Y	Y	Y
	Performance Information		Y		
vLoad Balancer	vLoad Balancer Installation	Y	Y		Y
	Network Configuration		Y		
	Resource Level		Y	Y	
	Contract Resources		Y		
	Routing	Y	Y	Y	Y
	Health Check	Y	Y	Y	Y
	Real Server Settings	Y	Y	Y	Y
	Server Group Settings	Y	Y	Y	Y
	VIP	Y	Y	Y	Y
	Monitoring	Y	Y	Y	Y
Global File Storage (Global Data Backup) Remote DC Storage (Japan) Remote DC Storage (Overseas)	Disk Capacity		Y		
	Boost Plan (S, M, L)		Y		
	Boost	Y	Y	Y	Y
	Replication	Y	Y	Y	Y

※1 File Backup Restore control is provided by the application installed in Virtual Machine.

※2 The function is available on the Customer Portal the service released Data Center. The number of Global IP address can be changed in case of using vFirewall.

※3 The function is available on the Customer Portal the service released Data Center.

※4 vApp is a new feature that can be seen on Customer Portal ver2.0 . vApp for Enterprise Cloud can only support one single Virtual Machine.

INFO

- For information about Virtual Machines, refer to "3
- Compute Resource" (⇒P.51).
- For information about Customer Portal features and how to use them, refer to the separate volume "Enterprise Cloud User's Guide."
- For information about the NTT Communications Business Portal, refer to the separate volume "Business Portal User's Guide."

2.1.3 Important Points

- The Customer Portal is accessed through a web browser using the Internet. Please prepare an environment in which you have Internet access.
- Use the following web browser to access the Customer Portal.

  Mozilla Firefox 10 or higher 32bit

  ※ To use a console connection, you need Mozilla Firefox 11.0 or higher running on Windows except version 8.
- If Firefox version is 30 or higher, please change VMware Remote Console Plug-in setting to be always activated.

NOTE

- NTT Communications is not responsible for unauthorized use of the Customer Portal resulting from the loss or leaking of password information issued to the customer.
- When using one Customer Portal to batch manage multiple Data Centers, please notify NTT Communications beforehand. You cannot consolidate Data Centers back into one Data Center after you start using them in separate Customer Portals.

INFO

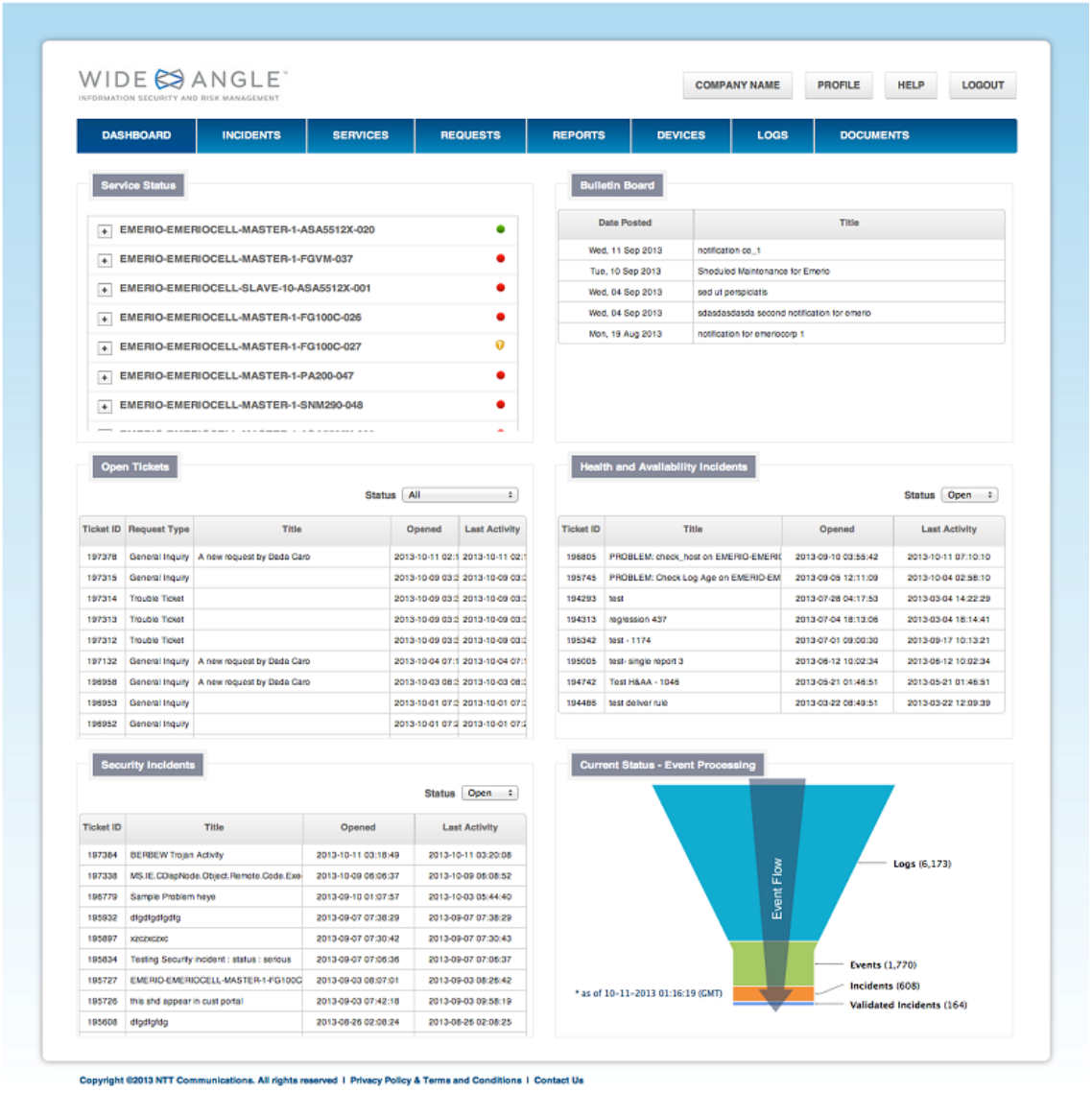
- When using a console connection, enable the Java Script features in your web browser.
- You cannot manage one Data Center from multiple Customer Portals.

2.2 Security Web Portal

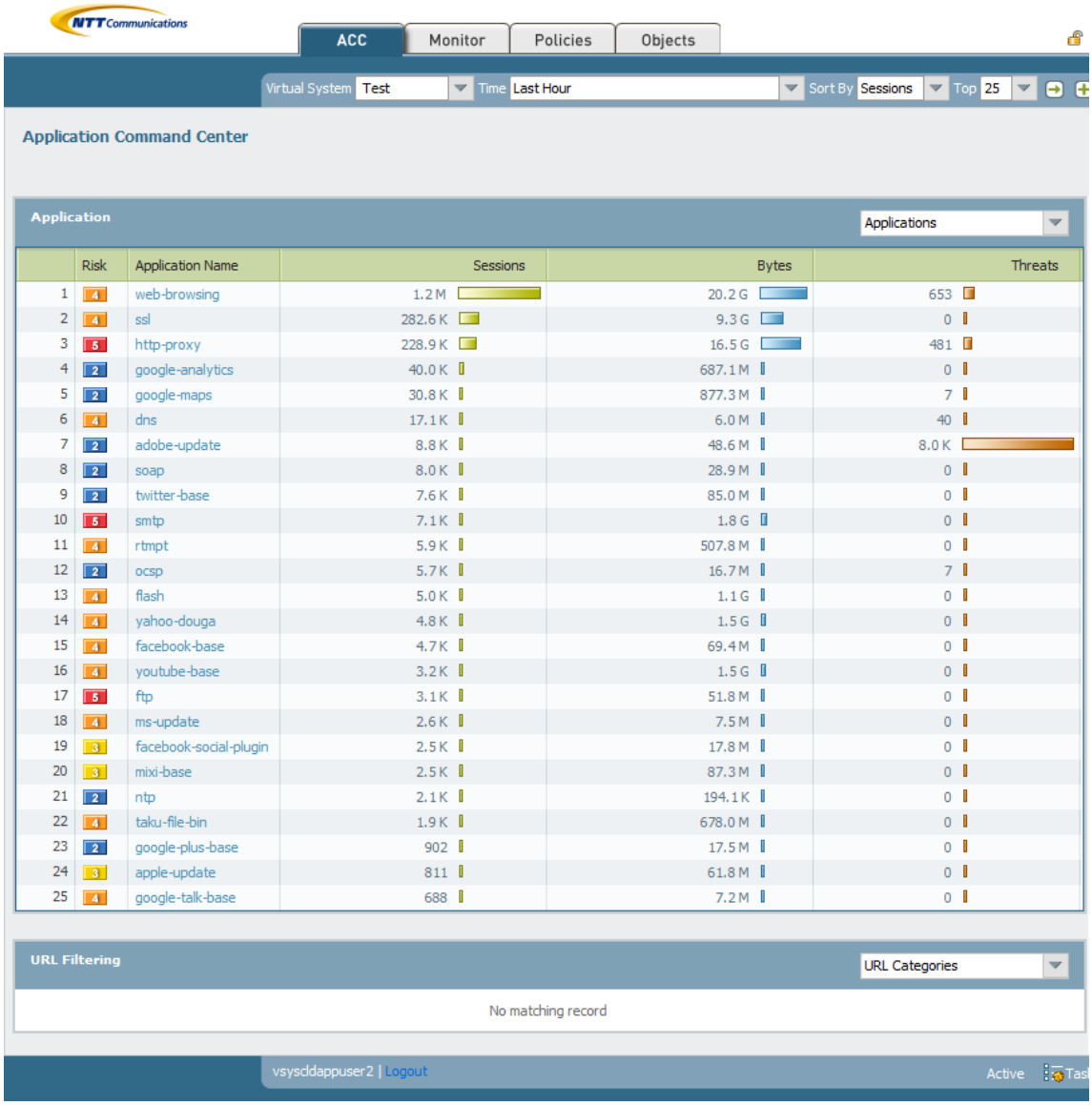
When you use Enterprise Cloud, you are provided with one administrator ID for the Security Web Portal, which can be used to check the status of attack trafficand unauthorized access attempts to a protected Server Segment.

The top pages of the Security Web Portal are shown below.

DCs outside Japan version (WideAngle MSS Customer Portal)



Japan DC version


NTT Communications
ACC
Monitor
Policies
Objects
Virtual System Test
Time Last Hour
Sort By Sessions
Top 25
Application Command Center
Application
Applications
Risk
Application Name
Sessions
Bytes
Threats
1 4 web-browsing 1.2 M 20.2 G 653
2 4 ssl 282.6 K 9.3 G 0
3 5 http-proxy 228.9 K 16.5 G 481
4 2 google-analytics 40.0 K 687.1 M 0
5 2 google-maps 30.8 K 877.3 M 7
6 4 dns 17.1 K 6.0 M 40
7 2 adobe-update 8.8 K 48.6 M 8.0 K
8 2 soap 8.0 K 28.9 M 0
9 2 twitter-base 7.6 K 85.0 M 0
10 5 smtp 7.1 K 1.8 G 0
11 4 rtmpt 5.9 K 507.8 M 0
12 2 ocsp 5.7 K 16.7 M 7
13 4 flash 5.0 K 1.1 G 0
14 4 yahoo-douga 4.8 K 1.5 G 0
15 4 facebook-base 4.7 K 69.4 M 0
16 4 youtube-base 3.2 K 1.5 G 0
17 5 ftp 3.1 K 51.8 M 0
18 4 ms-update 2.6 K 7.5 M 0
19 3 facebook-social-plugin 2.5 K 17.8 M 0
20 3 mixi-base 2.5 K 87.3 M 0
21 2 ntp 2.1 K 194.1 K 0
22 4 taku-file-bin 1.9 K 678.0 M 0
23 2 google-plus-base 902 17.5 M 0
24 3 apple-update 811 61.8 M 0
25 4 google-talk-base 688 7.2 M 0
URL Filtering
URL Categories
No matching record
vsysddappuser2 | Logout
Active

2.2.1 Available Features

Features in DCs outside Japan

You can use the following features in the Security Web Portal.

Feature	Overview
Service status	Displays devices status.
Bulletin Board	Displays maintenance notifications.
Open Tickets	Displays request tickets.
Health & Availability	Displays Health & Availability Incident tickets.
Service	Displays service status, devices, open requests, Health & Availability Incident tickets and open requests.

Requests	Displays request tickets and creates a new request.
Reports	Displays Device Management, Service Management and Security Management reports.
Device Information	Displays device and service information of the selected device. Displays request tickets and creates a new request.
Log Viewer	Allows users to view devices and logs. Also allows searching and downloading of logs.
Documents	Allows users to download user documents.

Features in Japan DC

Feature	Menu	Overview
ACC (Application Command Center)	IPS/IDS, Anti-Virus (E-mail, Web), Filtering (App, NW), Profiling (App, NW)	Displays the communication types and the status of use (e.g. bandwidth and sessions)
Monitor		Displays various kinds of logs and allows the user to download them.
Policies		Displays configured security policies.
Objects		Displays configured Address objects (host and network), Address object group. Displays application list, Antivirus profile list, anti-spyware profile list, vulnerability profile list, URL filitering profile list, configurable security policy.
Configuration Status	WAF	Displays status of Web service registered as the target and Web server used by the Web service.
Report Generation and and Display		Displays device status, allows user to generate and display various kinds of charts based on statistical information accumulated in the device. Displays the unauthorized access list.
Information of Signatures in staging		Displays the staging status and the list of signatures in staging.
Report Download		Allows users to download reports.
Policies	VM Security (VM Anti-Virus, VM Virtual Patch, VM Firewall)	Displays Security Policies. Displays configuration information.
Event Alert		Displays the events which VM security detected and allows the user to delete alerts.

Event Information		Displays the detailed information of events.
Report Generation and Download		Allows users to generate and download various kinds of report based on required period or host.
File Download		Allows users to download documents and installers.
Report Download	RTMD (Email, Web)	Allows users to download reports.

INFO

- Access to the Security Web Portal requires authentication using one-time password.

2.2.2 Important Points

- The Security Web Portal is accessed through a web browser using the Internet. Please prepare an environment in which you have Internet access.
- You cannot use the Security Web Portal (Japan DC version) to check information, such as maintenance and errors, for a period during which operations were being run on standby equipment.
- NTT Communications is not responsible for unauthorized use of the Security Web Portal resulting from the loss or leaking of password information issued to the customer.
- This system is different from the Enterprise Cloud Customer Portal.
- Security Web Portal (Japan DC version) will be intergrated into that of DCs outside Japan: WideAngle MSS Customer Portal.

3.Compute (Global Standard Menu)

3.1 Compute Resource

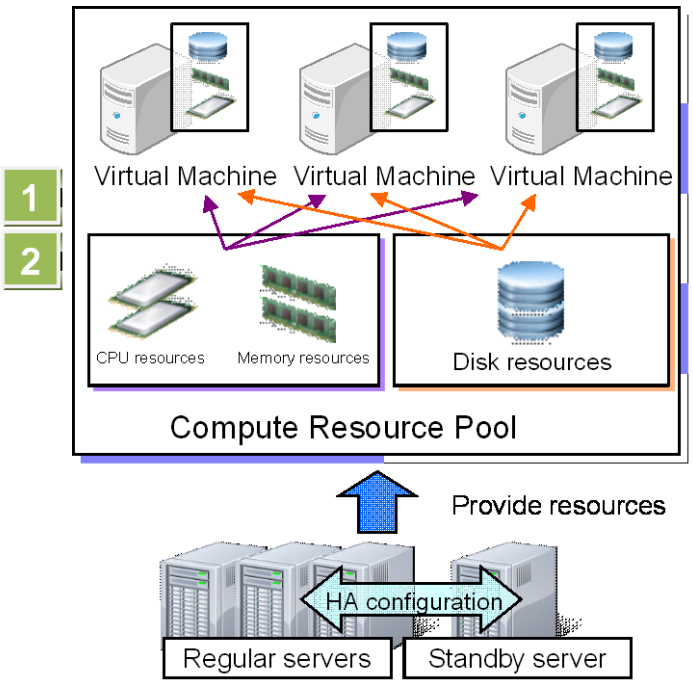
Compute Resource is a service that provides virtual equipment (Compute Resources) by combining CPUs, Memory, and Disks to create Virtual Machines. Compute Resources are provided by virtualizing physical servers and storage devices shared by multiple users.

Use the Customer Portal to create, change, or delete a Virtual Machine.

3.1.1 Available Features

You can use the following features in Compute Resource.

	Feature	Overview
1	Provision of Compute Resource Pools	A feature that uses the Compute Resources (CPU/Memory/Disk) to create Virtual Machines. You can create multiple machines.
2	Features for controlling Compute Resource Pools	From the Customer Portal, you can perform the following actions for Compute Resource Pools. ● Add/reduce resources ● Assign resources to a Virtual Machine ● Add, delete, or change a Compute Resource Pool



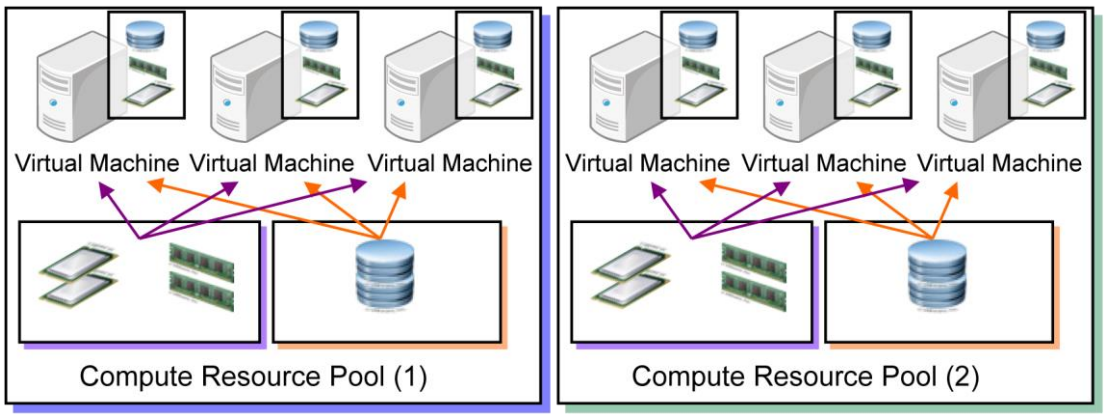
INFO

- The infrastructure for Compute Resources is comprised of HA (High Availability) clusters and storage devices that have spare physical servers. If a failure is detected on a physical server that contains Compute Resources, the server is automatically replaced by a standby server.
- You can select Compute Resources that offer the appropriate performance level (Guaranteed, Premium, Standard) for your intended use.

3.1.2 Provision of Compute Resource Pools

You can create and use multiple Compute Resource Pools (CPUs/Memory/Disk) to create a Virtual Machine.

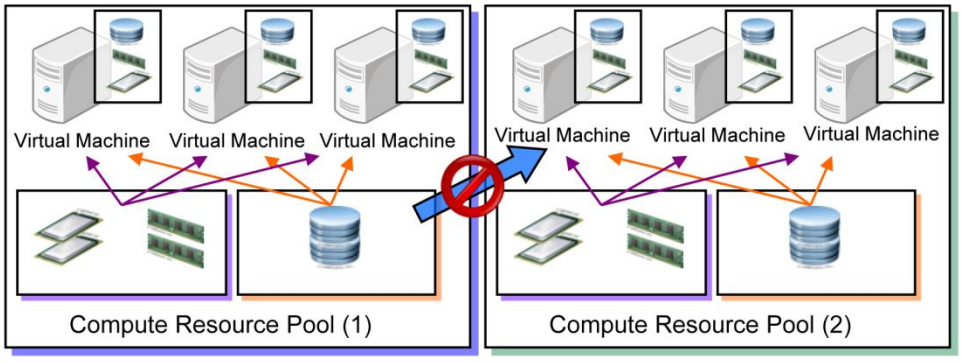
Use the Customer Portal to add, delete, and change Compute Resource Pools.



Adding a second resource pool

NOTE

- There must be at least one Compute Resource Pool.
- When using multiple Data Centers, there must be a Compute Resource Pool for each Data Center.
- Compute Resources (CPU/Memory/Disk) cannot be assigned to multiple Compute Resource Pools.



Usage Units

You can add or reduce the resources handled by one Compute Resource Pool within the ranges shown below.

Resource	Lower Limit	Upper Limit	Application Unit
CPU	1 GHz	48 GHz	1 GHz
Memory	1 GB	144 GB	1 GB
Disk	50 GB	4,000 GB	50 GB

You can add or reduce the resources assigned to one Virtual Machine within the ranges shown below. Configurable settings of Customer Portal ver1.0 are different from those of Customer Poral 2.0

For Customer Portal ver1.0

Resource	Lower Limit	Upper Limit	Application Unit
CPU	1	8	1vCPU
Memory	1 GB	32 GB	1 GB
Disk	1 GB	2,000 GB	1 GB

For Customer Portal ver2.0

Resource	Compute/ Storage	Lower Limit	Upper Limit	Application Unit
CPU	Guaranteed Compute	1	32	1 vCPU
	Premium Compute/ Standard Compute	1	8	1 vCPU
Memory	Guaranteed Compute	1 GB	128 GB	1 GB
	Premium Compute/ Standard Compute	1 GB	32 GB	1 GB
Disk	Premium Storage/ Standard Storage	1 GB	2,047 GB	1 GB
	Premium Storage/ Standard Storage	1 MB	2,097,151MB	1 MB

Classes

Compute Resource Pools are comprised of two types of classes: the Compute Class (CPU/Memory) and the storage class (Disks). Each of these is separated into two types of service classes (Premium and Standard) with different levels of performance. You can select the class that is appropriate for your intended use.

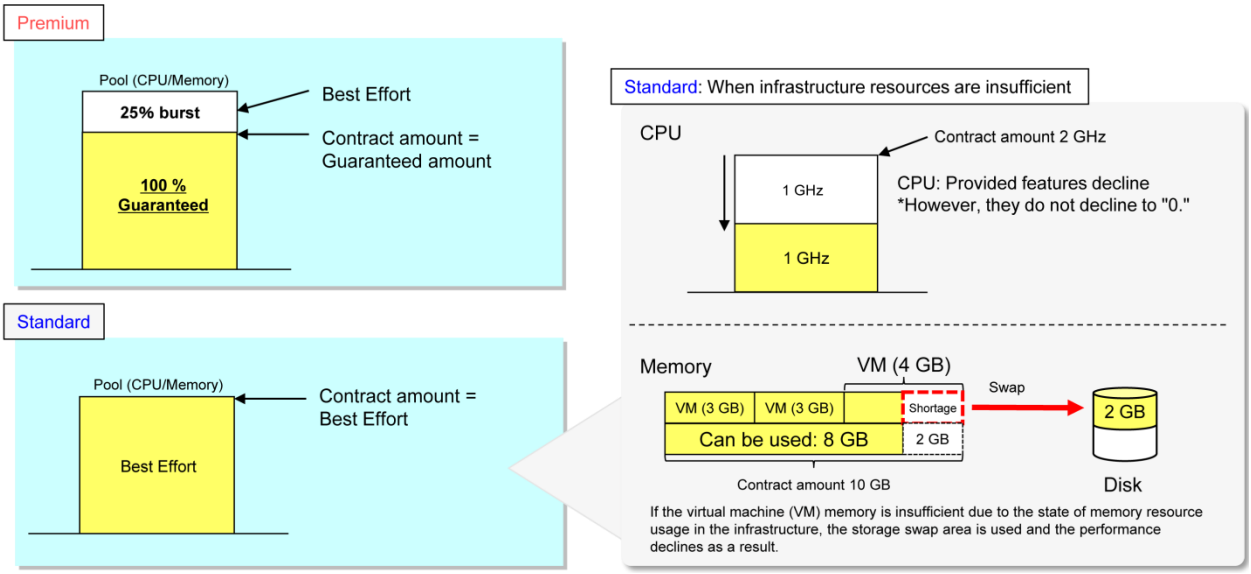
NOTE

- Select the service class when creating the Compute Resource Pool. You cannot change the service class after the Compute Resource Pool has been created.

Classes	Resource	Service Class	Details
Compute Class	CPU Memory	Guaranteed	The CPU resource and Memory resource values for which you applied are guaranteed. SLA is applicable for this component.
		Premium	The CPU resource and Memory resource values for which you applied are guaranteed.
		Standard	The CPU resource and Memory resource values for which you applied are provided on a best effort basis.
Storage Class	Disk	Premium	High-speed Disk performance is provided.
		Standard	Standard Disk performance is provided.

Compute Classes

The differences between compute service classes (Premium or Standard) are shown below.

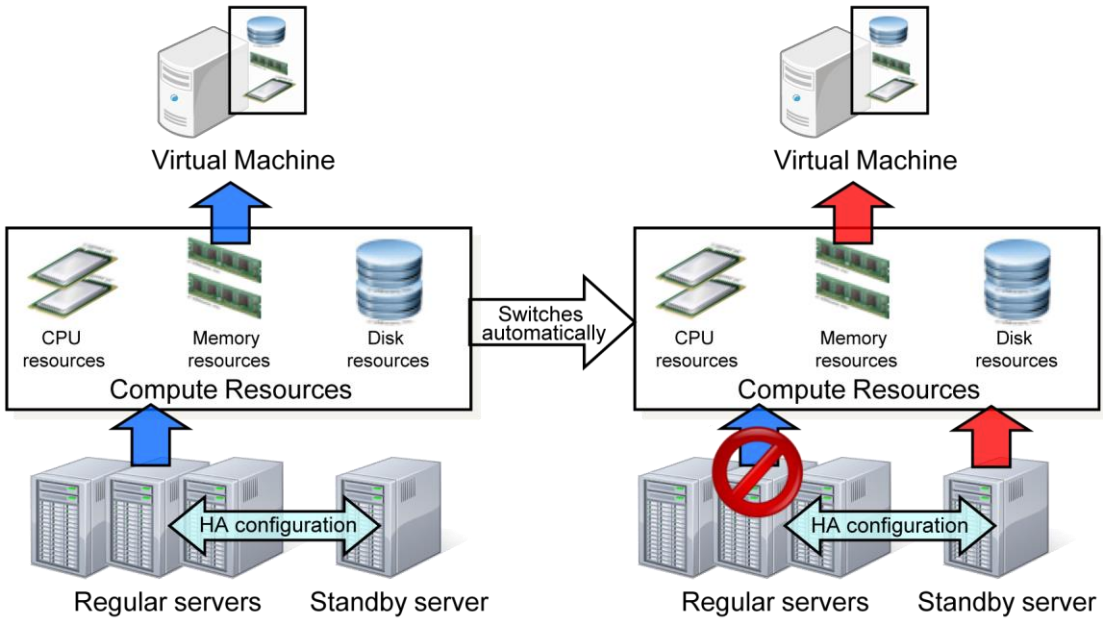


HA Cluster Feature

Compute Resources are comprised of storage devices and HA clusters that have more than one of the following two types of physical servers.

- Regular servers
- Standby servers (spare physical servers used for failure recovery)

When a failure is detected on a regular server, the HA Cluster feature automatically switches to the resources on a standby server (automatically recovers).



NOTE

- The HA Cluster feature does not detect any failures and perform an automatic recovery on a Virtual Machine that you have created.
- The HA Cluster feature does not guarantee the recovery of a Guest OS or applications running on a Guest OS, on a Virtual Machine that you have created.

Zones

When a failure is detected on a regular server, the Virtual Machine restarts on a standby server. The Virtual Machine that you created may temporarily stop until it restarts on the standby server.

As a result, if you have created a redundant configuration between multiple Virtual Machines but you have added the Virtual Machines to the same Compute Resource Pool, the redundant configuration may not behave as expected.

Zones are used to deal with this problem.

A zone is a group of physical equipment (physical servers and storage devices) that accommodates a Compute Resource Pool. You can choose either Zone A or Zone B for each Compute Resource Pool.

Virtual machines created from Compute Resource Pools with different zones run on different physical equipment, as shown below.

Example: When zones are set on Compute Resource Pools 1 to 3

Compute Resource Pool	Zone	Virtual Machine	Physical Equipment Running the Virtual Machine
Compute Resource Pool 1	Zone A	Virtual Machine i	Physical Equipment A
		Virtual Machine ii	Physical Equipment A
		Virtual Machine iii	Physical Equipment A
Compute Resource Pool 2	Zone A	Virtual Machine	Physical Equipment A
Compute Resource Pool 3	Zone B	Virtual Machine	Physical Equipment B

INFO

- For information on Data Centers that offer zones, refer to "1.3.2 Available Data Centers" (⇒P. 21).
- Zone function provides the availability of the physical serve that Virtual Macihne would run. It does not provide the availability for Network devices.

3.1.3 Features for Controlling Compute Resource Pools

From the Customer Portal, you can perform the following actions for Compute Resource Pools.

Feature	Overview
Add/reduce resources	A feature for adding and reducing the three types of resources (CPU/Memory/Disk) in a Compute Resource Pool.
Assign resources to a Virtual Machine	A feature for assigning Compute Resources (CPU/Memory/ Disk) to a Virtual Machine created in a Compute Resource Pool.
Add or delete a Compute Resource Pool	A feature for adding or deleting a Compute Resource Pool.

3.1.4 vApp Feature

vApp is a new feature that can be seen on Customer Portal ver2.0 . vApp is a container for Virtual Machines which is managed by VMware.All functional characteristics of vApp is currently not supported in Enterprise Cloud.vApp for Enterprise Cloud can only support one single Virtual Machine.

3.1.5 Assigning Resources to a Virtual Machine

Create a Virtual Machine by assigning resources in a Compute Resource Pool (CPUs/Memory/Disk) to the Virtual Machine. The amount of resources that can be assigned to a Virtual Machine is different with Customer Portal ver1.0 and Customer Portal ver2.0 .

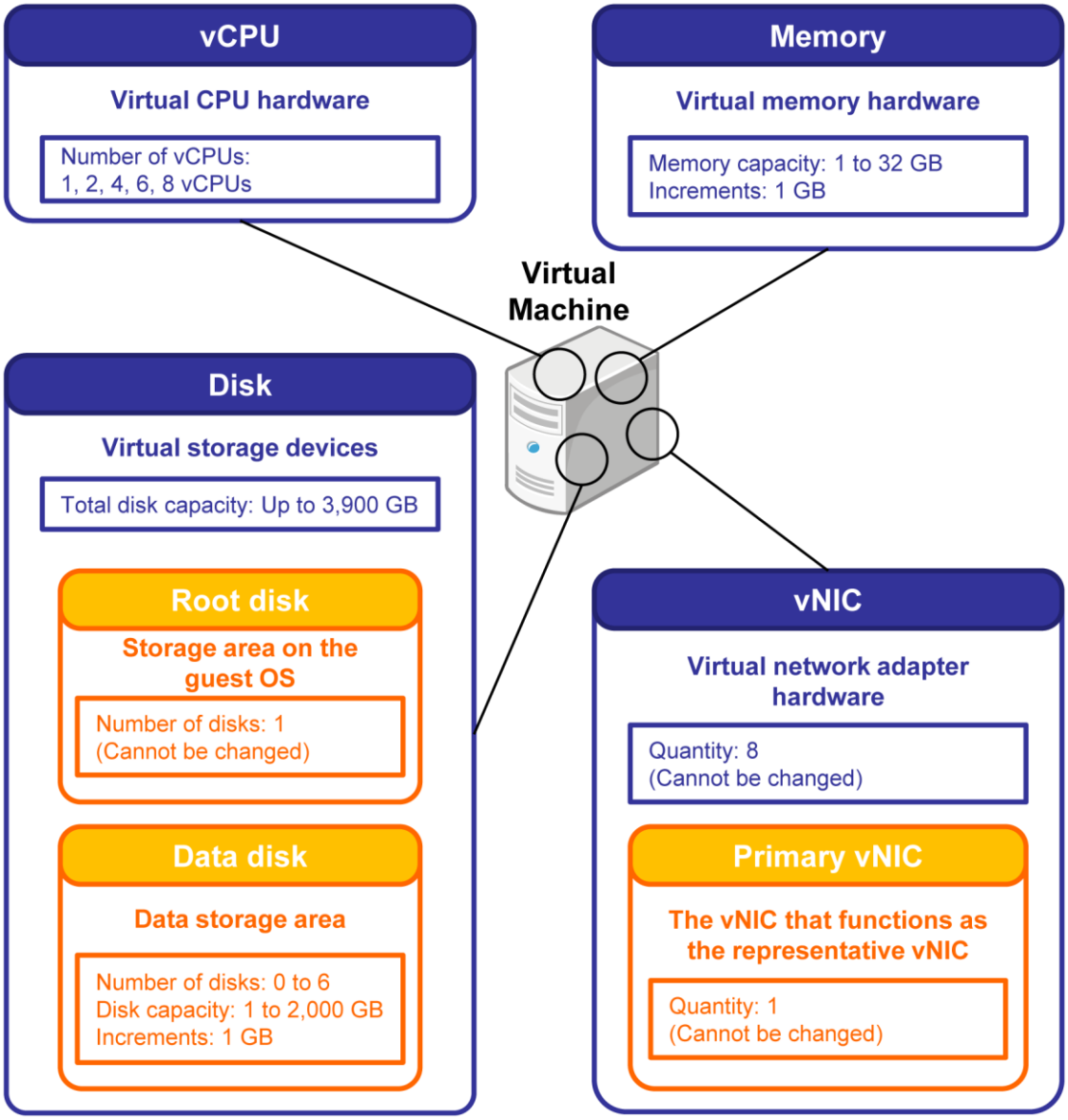
You can also add or reduce resources for the Virtual Machine once you have created it.

INFO

- The number of Virtual Machines that you can create depends on the number of contracted resources and the number of private IP addresses that can be used on a Server Segment. IP addresses are used for vFirewall, vLoad Balancer, Service Interconnectivity, and Virtual Machines. You can verify usage in the portal.

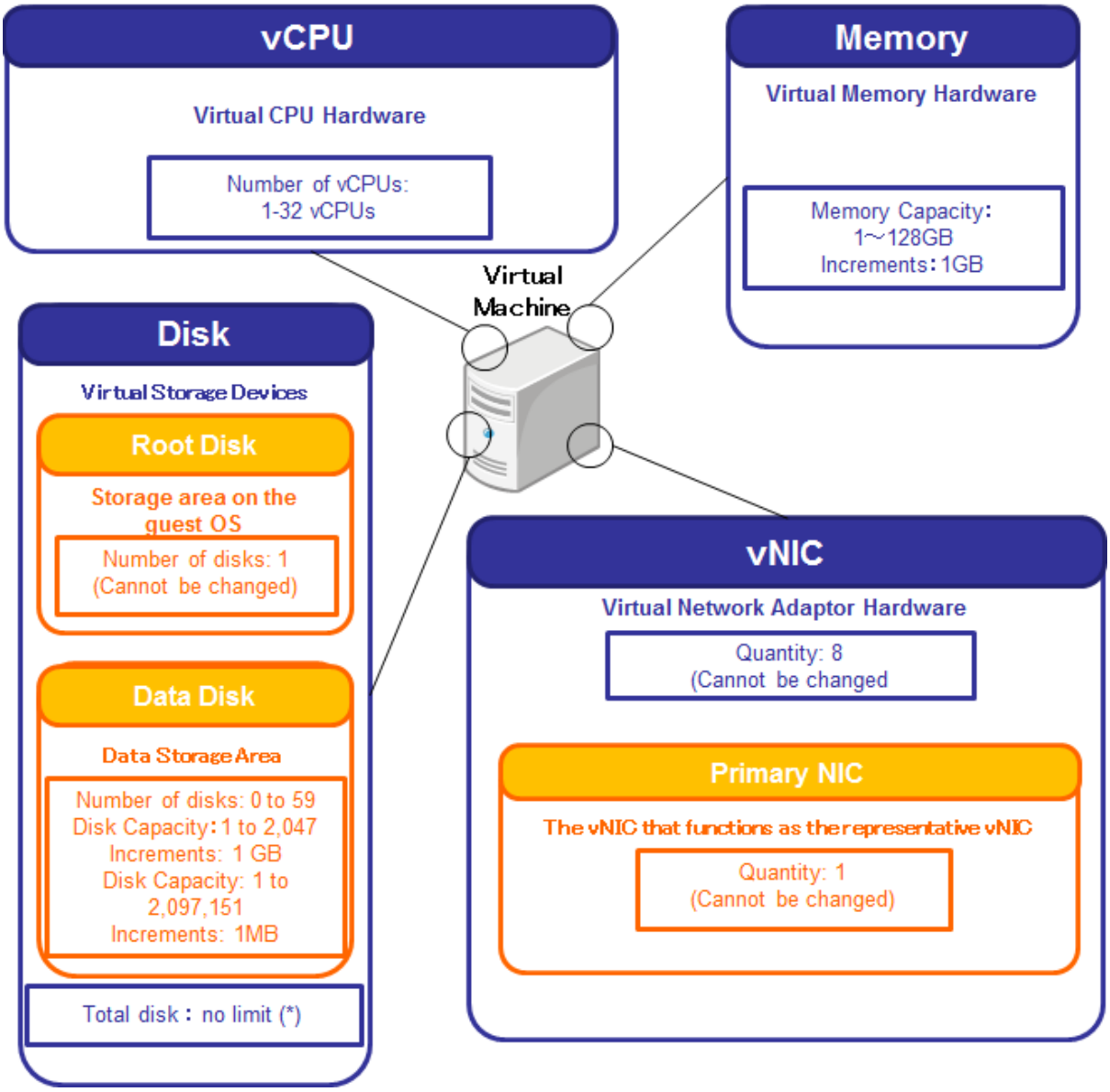
Virtual machines are made up of six components (vCPU/Memory/Disk/vNICs/Virtual CD/DVD drives/Guest OS).

Resources that can be assigned to a Virtual Machine (Customer Portal ver1.0)



Resources that can be assigned to a Virtual Machine (Customer Portal ver2.0)

*The amount of resources that can be assigned to Virtual Machine differ according to the Compute Class.



* Total disk capacity (no limit) + Memory capacity (different for each Compute Class) must be less than the amount of space left in storage

vCPU

A vCPU is virtual CPU hardware that makes up a Virtual Machine.

From the Compute Resource Pool, you can specify the number of vCPUs and assign it to a Virtual Machine.

How many can be assigned?

The quantities of vCPUs that can be assigned to one Virtual Machine are shown below. The configurable setting of Customer Portal ver1.0 are different from those of Customer Portal ver2.0 .

Customer Portal ver1.0

Service Menu	Compute Class	Min	Max	Step
Compute Resource (Shared Device)	Guaranteed	1	8	※
	Premium	1	8	※
	Standard	1	8	※

※Configurable value of vCPUs are 1,2,4,6,or 8. Odd number vCPUs cannot be configured on Customer Portal ver1.0 .

Customer Portal ver2.0

Service Menu	Compute Class	Min	Max	Step
Compute Resource (Shared Device)	Guaranteed	1	32	1
	Premium	1	8	1
	Standard	1	8	1

NOTE

- You can only change the number of vCPUs when the Virtual Machine is powered off. Please do not change configuration in Partially Powered Off state.

vCPU processing capacity

The vCPU processing capacity is different for each Data Center. The processing capacity is the same as the physical processors listed in the table below.

Data Center	Processor
Yokohama No.1	2010 Intel Xeon Processor (equivalent to a maximum of 2.5 GHz)
Kansai 1	2012 Intel Xeon Processor (equivalent to a maximum of 2.0 GHz)
Saitama No.1	2012 Intel Xeon Processor (equivalent to a maximum of 2.2GHz)
Hong Kong Tai Po	2009 Intel Xeon Processor (equivalent to a maximum of 2.7 GHz)

Singapore Serangoon	2012 Intel Xeon Processor (equivalent to a maximum of 2.2 GHz)
San Jose Lundy	2012 Intel Xeon Processor (equivalent to a maximum of 2.2 GHz)
Virginia Sterling	2012 Intel Xeon Processor (equivalent to a maximum of 2.2 GHz)
UK Hemel Hempstead2	2012 Intel Xeon Processor (equivalent to a maximum of 2.2 GHz)
Thailand Bangna	2012 Intel Xeon Processor (equivalent to a maximum of 2.0 GHz)
Malaysia Cyberjaya3	2012 Intel Xeon Processor (equivalent to a maximum of 2.2 GHz)
Australia Sydney1	2012 Intel Xeon Processor (equivalent to a maximum of 2.2 GHz)
Germany Frankfurt2	2012 Intel Xeon Processor (equivalent to a maximum of 2.2 GHz)

NOTE

- The vCPU processing power varies depending on the following conditions. There is no guarantee that a vCPU will always operate at the maximum processing capacity.
  - When the total vCPU processing capacity for Virtual Machines running in one Compute Resource Pool is more than the purchased Compute Resource Pool (CPU resources)
  - The load condition of the Guest OS on the Virtual Machine

Understanding resource consumption

The CPU resources that are consumed from the Compute Resource Pool are the resources that are actually used by the Virtual Machine for computational processing.

INFO

- If a vCPU assigned to a Virtual Machine is not running, CPU resources are not consumed from the Compute Resources.
- If computational processing by a vCPU reaches the CPU upper limit for the Compute Resource Pool for each Virtual Machine, the processing capacity is averaged between the Virtual Machines and operations continue.

Memory

Memory is virtual Memory hardware that makes up a Virtual Machine.

From the Compute Resource Pool, you can specify the Memory capacity and assign capacity to a Virtual Machine.

How many can be assigned?

You can add or reduce the Memory capacity that is assigned to one Virtual Machine within the ranges shown below. The configurable settings of Customer Portal ver1.0 are different from those of Customer Portal ver2.0 .

Customer Portal ver1.0

Service Menu	Compute Class	Min	Max	Step
Compute Resource (Shared Device)	Guaranteed	1	8	1
	Premium	1	8	1
	Standard	1	8	1

Customer Portal ver2.0

Service Menu	Compute Class	Min	Max	Step
Compute Resource (Shared Device)	Guaranteed	1	128	1
	Premium	1	32	1
	Standard	1	32	1

NOTE

- You can only change the Memory capacity when the Virtual Machine is powered off. Please do not change configuration in Partially Powered Off state.

Understanding resource consumption

The capacity totals below are consumed from the Compute Resource Pool.

- Total Memory capacity set for Virtual Machines that are running
- Memory resources for virtualization overheads

For information regarding overheads, refer to "3.1.6 Important Points" (⇒P.69).

NOTE

- The available Memory capacity varies depending on the following situations. There is no guarantee that the maximum Memory capacity will be always available.
  - The usage status of Memory resources for which you have applied
  - The load condition of the Guest OS on the Virtual Machine

INFO

- When the Memory resources consumed on each Virtual Machine reach the upper limit of Memory for the Compute Resource Pool, Memory in the swap regions of the Disk resources may be activated.

Disk

A Disk is a virtual storage device that makes up a Virtual Machine.

From the Compute Resource Pool, you can specify the Disk capacity and assign capacity to a Virtual Machine.

There are two types of Disks: a root Disk and a data Disk.

Disk	Description
Root Disk	The Disk that stores the Guest OS. There is always one root Disk created for one Virtual Machine.
Data Disk	The Disk that stores data. You can connect multiple Disks for one Virtual Machine.

NOTE

- If a Virtual Machine is deleted, the root Disk and data Disks are deleted at the same time.
- The data from a deleted Disk is erased according to the appropriate method specified by NTT Communications. A data erasure certificate is not issued.
- You cannot remove (detach) a data Disk that is connected to a Virtual Machine and connect (attach) it to another Virtual Machine.

INFO

- You can add and delete data Disks and expand the Disk capacity from the Customer Portal, regardless of whether the Virtual Machine is powered on or off. But please do not change in Partially Powered Off state.
- If you add or delete a data Disk or expand the Disk capacity while the Virtual Machine is powered on, the Disk may not be recognized properly by the Guest OS. However, it will be recognized properly if the Guest OS is compatible with hot swap.
- The Disk capacity of the root Disk depends on the template that was selected when creating the Virtual Machine.

How many can be assigned?

You can add or reduce the Disk capacity and the number of data Disks connected to one Virtual Machine within the ranges shown below. The configurable settings of Customer Portal ver1.0 are different from those of Customer Portal ver2.0 .

Customer Portal ver1.0

	Lower Limit	Upper Limit	Setting Unit
Number of data Disks	0	6	1

Disk capacity	1 GB	2,000 GB	1 GB

Customer Portal ver2.0

	Lower Limit	Upper Limit	Setting Unit
Number of data Disks	0	59	1
Disk capacity	1 GB	2,047 GB	1 GB
	1 MB	2,097,151 MB	1 MB

INFO

- There is no limit for total disk capacity. However, the total disk capacity (no limit) + Memory Resource (different for each Compute Class) must be below the amount of space left in storage resource.

Understanding resource consumption

The capacity totals below are consumed from the Compute Resource Pool.

- Total Disk capacity assigned to a Virtual Machine
- Capacity of swap regions for each Virtual Machine (same capacity as the Memory capacity)

vNIC

A vNIC is virtual network adapter hardware that makes up a Virtual Machine.

The Server Segment service provides an L2 connection to Server Segments in the same Data Center.

NOTE

- A separate application is required to use the Server Segment service.
- One of the assigned vNICs must be set as the representative vNIC (called the "Primary vNIC" below). Some of the initial settings for the Guest OS are affected by the primary vNIC selection. For details, refer to the Enterprise Cloud User's Guide, "2.4.1.4 Initial Settings For Virtual Machines."
- Monitoring of Virtual Machine pings is performed for the primary vNIC.

INFO

- You can specify settings for an L2 connection between a primary vNIC and a Server Segment only when creating a Virtual Machine or when the Virtual Machine is powered off. Specify the settings from the Customer Portal.
- You cannot connect multiple vNICs from the same Virtual Machine to one Server Segment.

How many can be assigned?

Eight vNICs can be used on one Virtual Machine. This cannot be changed. The configurable settings of Customer Portal ver1.0 and Customer Portal ver2.0 are the same.

INFO

- You can assign IP addresses to vNICs when creating a Virtual Machine. You can also change the IP address that is assigned to a vNIC.
- The system can automatically assign an IP address to a vNIC. To use this option, select Auto Assign.
- The system can automatically assign the IP address to vNIC from the available IP addresses in the IP address block specified by the Server Segment. You can also set an IP address from the Customer Portal.
- Sub-interface settings other than the IP addresses assigned to vNICs are specified on the Guest OS. To change an IP address in the sub-interface settings, you must first register the IP address that you want to assign as a reserved IP.

Virtual CD/DVD Drive

A virtual CD/DVD drive is virtual CD/DVD-ROM drive hardware that makes up a Virtual Machine.

NOTE

- You can connect only one virtual CD/DVD drive to one Virtual Machine. The number of virtual CD/DVD drives cannot be changed.

Guest OS

Only Guest OSes that are supported by vCloud Director can be used with Virtual Machines. The Guest OSes that are supported by vCloud Director are the Guest OSes marked as "Automatic" in the "Customization Support" column under "Guest OS Support" in the document below.

https://www.vmware.com/files/jp/pdf/vCloud_Director_User_Guide_15_jp-ja.pdf

NOTE

- Install and enable the latest VMware Tools in the Guest OS on the Virtual Machine. If you intentionally uninstall or disable VMware Tools, we cannot guarantee the correct operation of Compute Resources. We also may not be able to support your queries.

Guest OS Customization

Guest OS settings basically depend on the template. However, some settings are automatically changed after power on at the first time in following operation. This is referred to as Guest OS customization.

1) After creating a Virtual Machine
2) After changing the Server Segment to which a vNIC connects
3) After changing the primary vNIC
4) After changing the IP address of the vNIC

NOTE

- The Virtual Machine automatically restarts when the Guest OS is customized. Do not log in to the Guest OS or operate the Virtual Machine until it has restarted. The Virtual Machine will operate in the state that it was in prior to customization of the Guest OS, until it restarts.
- Please do not operate Virtual Machine during Guest OS Customization. Usually, it takes about 30 minutes.

Settings that are changed when customizing the Guest OS

The Guest OS settings that are changed when customizing the Guest OS are shown below.

■Items that are changed automatically when turning the power on for the first time after creating a Virtual Machine.

Item	Setting	Remarks
IP Address	A value specified by the user or by NTT Communications	Applies to all vNICs.
Net mask	The subnet mask of the Server Segment to which the vNIC connects	Applies to all vNICs.
Default gateway	A value specified by the user or by NTT Communications (※)	
Primary DNS	A value specified by the user or by NTT Communications	
Secondary DNS	A value specified by the user or by NTT Communications	
DNS suffix	A value specified by the user or no value	
S-ID	-	For Windows OS only, a Sysprep is performed and the S-ID is changed automatically.
root/Admin password	A value specified by NTT Communications	
Host/computer name	A value specified by NTT Communications	

※ The settings that are specified by NTT Communications are the IP addresses for the vFirewall/Integrated Network Appliance for the Server Segments to which the primary vNIC connects. However, the IP address that is set for Server Segments that do not connect to the vFirewall/Integrated Network Appliance is "the "broadcast address" of the IP address block for the Server Segment - 1." For example, if the IP address block is "192.168.0.0/24," the IP address that is "the "broadcast address" of the IP address block for the Server Segment - 1" will be "192.168.0.254."

■Settings that are changed automatically when starting for the first time after changing the Server Segment to which the vNIC connects, the primary vNIC, or the vNIC IP address

Item	Setting	Remarks
IP Address	A value specified by the user or by NTT Communications	Applies to the vNIC for which the destination Server Segment has changed.
Net mask	The subnet mask of the Server Segment to which the vNIC connects	Applies to the vNIC for which the destination Server Segment has changed.
Default gateway	A value specified by the user or by NTT Communications (※)	
Primary DNS	A value specified by the user or by NTT Communications	
Secondary DNS	A value specified by the user or by NTT Communications	
DNS suffix	A value specified by the user or no value	
Host/computer name	A value specified by NTT Communications	

※ The settings that are specified by NTT Communications are the IP addresses for the vFirewall/Integrated Network Appliance for the Server Segments to which the primary vNIC connects. However, the IP address that is set for Server Segments that do not connect to the vFirewall/Integrated Network Appliance is "the "broadcast address" of the IP address block for the Server Segment - 1." For example, if the IP address block is "192.168.0.0/24," the IP address that is "the "broadcast address" of the IP address block for the Server Segment - 1" will be "192.168.0.254."

INFO
- The S-ID and root/Admin password does not change.

■Contents that are automatically changed at the initial start after restoring the Image Backup

Item	Setting value	Remarks
Net Mask	Subnet mask of the the server segment to which the vNIC is connected	Applies to all vNICs.
Gateway	Value specified by customer or NTT Communications *1	
Primary DNS	Value specified by customer or NTT Communications	
Secondary DNS	Value specified by customer or NTT Communications	
DNS suffix	Value specified by customer or no value	
Host mame/ Computer name	Value specified by NTT Communications	

※ 1. The values specified by NTT Communications are the IP addresses for the vFirewall/Integrated Network Appliance for the Server Segments to which the primary vNIC connects. However, the IP address that is set for Server Segments that do not connect to the vFirewall/Integrated Network Appliance is "the "broadcast address" of the IP address block for the Server Segment - 1." For example, if the IP address block is "192.168.0.0/24," the IP address that is "the "broadcast address" of the IP address block for the Server Segment - 1" will be "192.168.0.254."

INFO

- IP address, root/Admin password, mac address are restored with values upon backup. Other parameters are changed to the setting values described in the above table. Note that parameters which changed in Guest OS are not recovered.
- S-ID is not changed.

3.1.6 Important Points

Resources Consumed by the Memory And Disk Overhead Regions In Connection With Server Virtualization

Virtual machines have four types of power states. The consumption of resources in the overhead regions for server virtualization depends on the power state. The overheads therefore need to be taken into account when designing the system (designing resources).

Each power state and the overhead regions required for each power state are shown in the table below.

The items marked with a "Y" are items that consume resources in overhead regions. For example, if the power state is Powered Off, resources from the overhead are not consumed for the CPU and Memory. On the other hand, the overhead portion consumes resources for the Disks.

Power State	Meaning of Power State	CPU	Memory (※1)	Disk (※2)
Powered Off	The power for the Virtual Machine is off.	-	-	Y
Partially Powered Off	The power for the Virtual Machine is on but the Guest OS is stopped.	-	-	Y
Powered On	The power for the Virtual Machine is on.	Y	Y	Y
Suspended	The operation of the Virtual Machine has been stopped temporarily using the cloud infrastructure. The suspend state and sleep state for the Guest OS is different to hibernation.	-	-	Y

※1 The following overhead regions are required based on the number of vCPUs.

Memory resource overheads (reference values)

Memory OH(MB)		Memory set on VM (GB)									
		1	2	4	8	16	32	64	128	256	512
vCPU	1	27.01	33.55	46.68	69.79	122.31	230.52	443.3	860.93	1699.84	3389.44
	2	33.63	40.16	53.29	75.28	126.39	237.13	447.23	870.77	1710.08	3389.44
	4	46.86	53.4	66.53	92.79	145.32	250.37	460.46	880.67	1730.56	3409.92
	8	61.33	79.87	93	119.26	171.79	276.84	486.93	907.16	1751.04	3440.64
	16	102.27	108.8	145.93	172.2	224.72	279.75	539.87	960.13	1802.24	3491.84
	32	150.33	153.74	169.99	222.38	309.28	401.83	611.93	966.04	1904.64	3553.28

※2 The capacity of Disk resources consumed as the swap region is the same as the used Memory capacity.

Used IP Addresses

- Allocate one Server Segment IP address block to one Server Segment and specify the prefix length. Specify a prefix length of /29 to /24 for each Server Segment.
- NTT Communications manages the allocated IP address block for the Server Segment, and assigns the IP address selected from the IP address block to each

device that connects to that Server Segment. For details, please check the description of features for each service.

- In the IP address block for the Server Segment, you cannot specify overlapping IP addresses across the following address bands.

Data Center	Non-duplicatable IP Address Bands
Yokohama No.1	172.22.0.0/17 172.22.128.0/17 10.223.0.0/17 10.223.128.0/17
Kansai 1	172.23.0.0/17 172.23.128.0/17 10.233.0.0/17 10.233.128.0/17
Saitama No.1	172.27.0.0/16 10.237.0.0/16 10.238.0.0/16
Hong Kong Tai Po	172.22.128.0/17 172.31.128.0/17 10.223.128.0/17 10.224.128.0/17
Singapore Serangoon	172.20.0.0/17 172.20.128.0/17 10.200.0.0/17 10.200.128.0/17
Germany Frankfurt2	172.22.0.0/16 10.223.0.0/16
San Jose Lundy Virginia Sterling UK Hemel Hempstead2 Thailand Bangna Malaysia Cyberjaya3 Australia Sydney1	172.22.0.0/17 172.22.128.0/17 10.223.0.0/17 10.223.128.0/17

NOTE

- The IP address block for the Server Segment cannot be changed after it is allocated.

Restrictions on the Hardware Configuration for Compute Resource

- If multiple Virtual Machines with the same role are created for one physical server and that physical server fails, the applications on those Virtual Machines may stop at the same time.
- You cannot select a physical server that runs a specific Virtual Machine.
- The network equipment and physical server interface provided by Compute Resource has redundancy. If the interface fails, it automatically switches from the regular interface to the standby interface. The Guest OS on the Virtual Machine and the applications that are running on the Guest OS may be affected when switching interfaces.
- If the zone is the same, resources may be kept on the same physical server or storage device, even if the service class (Premium or Standard) is different.

Restrictions on the Settings for Compute Resource Application Resources

- The performance of each resource may vary by Data Center.
- When changing Compute Resources, you need to create the Virtual Machines and configure the resource settings for Virtual Machines yourself. NTT Communications is not responsible for errors that occur as a result of these settings, such as abnormal operation of your applications.

NOTE
- When changing Compute Resources, we may ask you to create a new Compute Resource Pool to ensure that a stable service is provided, even if the compute resource that you are changing has not reached the resource upper limits.

Restrictions on Virtual Machine Disks

- To use the Disk capacity expansion feature, you need to install and enable VMware Tools (Version 8.6.0 or higher) in the Guest OS on the Virtual Machine.
- The Disk capacity expansion feature cannot be used while a backup image is being obtained.

NOTE
- You cannot reduce the Disk capacity.

Restrictions on Virtual Hardware

- You cannot change MAC addresses that have been set on virtual hardware such as vNIC.
- You cannot use your own MAC addresses that are not administered by NTT Communications.
- If we become aware that you have changed a MAC address or are using your own MAC address, we may stop that Virtual Machine without advance notice.

Restrictions on the Guest OS and Applications

- When installing a Guest OS on a Virtual Machine, you need to verify the system requirements for the Guest OS (number of vCPUs, Memory capacity, Disk capacity, and so on), licenses, and terms of support with your Guest OS vendor yourself.
- When installing applications on a Guest OS, you need to verify the system requirements for the application (number of vCPUs, the CPU processing capacity of the vCPU, Memory capacity, number and capacity of Disks, number of vNICs, and so on), licenses, and terms of support with your application vendor yourself.
- When you install a Guest OS or application, NTT Communications is not responsible for checking or reporting whether operations can be guaranteed in your system configuration or whether there are any licensing issues.
- The Guest OS will recognize a vNIC as a NIC, even if it is not connected to a Server Segment. When changing the Guest OS network settings, do not disable a vNIC that has been recognized, even if you are not using that vNIC. If you do disable it, errors may occur in services such as Private Catalog and Image Backup.

Other

- Compute Resource uses software that NTT Communications has licensed from VMWare, Inc.
- The VMware features provided in Compute Resource have been selected based on Compute Resource specifications. Not all VMware features are included.
- The following virtualization software is used in Compute Resource.
  - VMware vSphere
  - VMware vCloud Director
  - Equivalent successor products

3.2 Compute Resource (Dedicated Device)

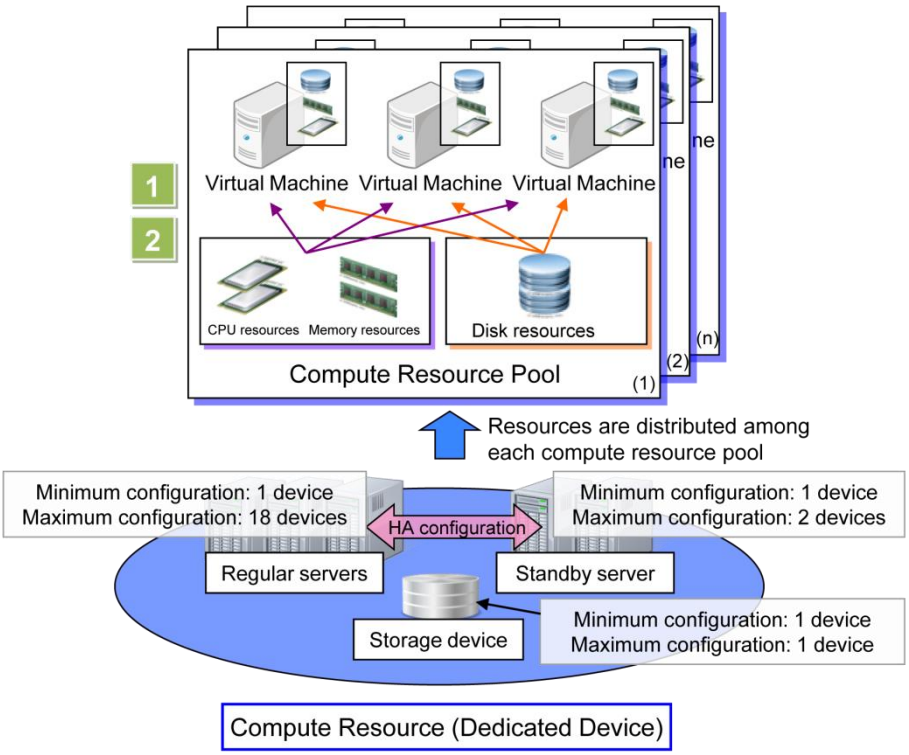
Compute Resource (Dedicated Device) is a service that provides virtual equipment (Compute Resources) by combining CPUs, Memory, and Disks to create Virtual Machines. Compute Resources are provided by virtualizing physical servers and storage devices within a physical enclosure dedicated to you.

You can use multiple dedicated devices in the Data Center that you are using.

3.2.1 Available Features

You can use the following features in Compute Resource (Dedicated Device).

	Feature	Overview
1	Provision of Compute Resource Pools	You can create and use multiple Compute Resource Pools (CPU/Memory/Disk) to create a Virtual Machine. However, in Compute Resource you use your own dedicated physical servers and storage devices provided by NTT Communications.
2	Features for controlling Compute Resource Pools	You can perform the following actions for Compute Resource Pools. ● Specify the values (reserved values) to guarantee CPU, Memory, and Disk resources ● Specify the percentage of the reserved value (reserved rate) for the upper limits (limit values) and the limit values of available CPU and Memory resources ● Add, delete, or change a Compute Resource Pool



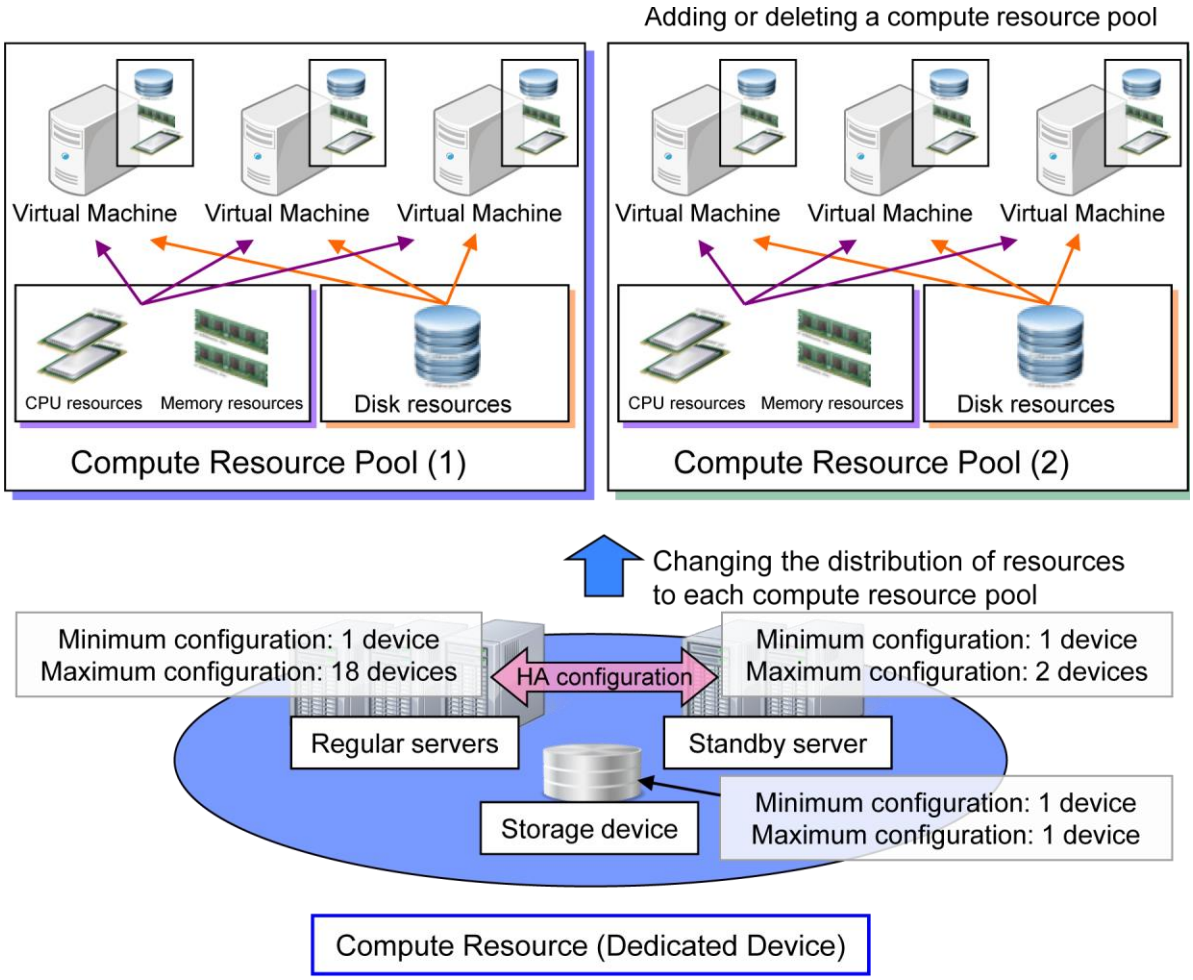
INFO

- Compute Resource (Dedicated Device) is a service that provides the same features as Compute Resource, the service in which physical equipment is shared with other users. This section explains the differences between the two services. For information regarding Compute Resource, refer to "3
- Compute Resource" (⇒P.51).
- You can select storage devices from a storage class (Premium or Premium+) that offers the appropriate performance level for your intended use.

3.2.2 Provision of Compute Resource Pools

In Compute Resource (Dedicated Device), you can use Compute Resources (CPU/Memory/Disk) that are comprised of your own dedicated physical servers and storage devices provided by NTT Communications. In addition, you can divide your Compute Resources into multiple Compute Resource Pools.

To add, delete, or change a Compute Resource Pool, please submit the application specified separately.



NOTE

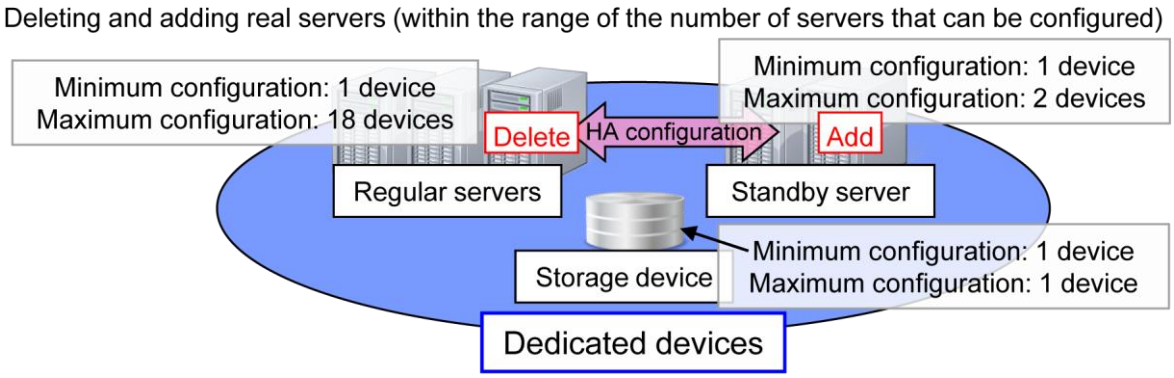
- You may not be able to add, delete, or change a Compute Resource Pool, depending on the compute resource usage conditions.

Usage Units

You can add or reduce the physical servers (regular servers and standby servers) and storage devices handled by dedicated devices within the ranges shown below.

To add, delete, or change a physical server, please submit the application specified separately.

Dedicated Device	Lower Limit	Upper Limit	Application Unit
Regular servers	1	18	1
Standby server	1	2	1
Storage device	1	1	-



NOTE

- In Compute Resource (Dedicated Device), the physical server is combined with an HA cluster configuration. You therefore need a total of two servers, one regular server and one standby server, as the minimum configuration for one dedicated device.
- You may not be able to add or delete a physical server, depending on the compute resource usage conditions.

The amount of resource that could be distributed to each compute resource pool from the dedicated device is as follows.

Resource	Minimum	Maximum	Unit
CPU	1 GHz	Total amount of CPU resource of HA Cluster [Active Server]	1 GHz
Memory	1 GB	Total amount of Memory resource of HA Cluster [Active Server]	1 GB
Disk	50 GB	Disk resource of Storage Device	50 GB

メモ

- There is no limit for total disk capacity. However, the total disk capacity (no limit) + Memory Resource (different for each Compute Class) must be below the amount of space left in storage resource.

ClassesThe Compute Resource Pool is comprised of two classes: a Compute Class (CPU and Memory) provided by a physical server, and a storage class (Disks) provided by a storage device. You can choose from three different service class (Small/Medium/Large) that has differenct resource capacity.Storage classes are separated into two types of service classes (Premium and Premium+) with different levels of Disk performance. You can select the class that is appropriate for your intended use.

Classes	Resource	Service Class	Details
Compute Class (Physical server)	CPU Memory	Small	The Physical Server of Small is the smallest. The physical server of Small provides smaller CPU Reource and Memory Resource than Medium.
		Medium	The Physical Server of Medium is larger than that of Small and smaller than that of Large. The physical server of Medium provides larger CPU Reource and Memory Resource than Small.
		Large	The Physical Server of Large is the largest. The Physical Server of Large provides the largest CPU Resource and Memory. The CPU performance iof Lrge is higher than that of Medium.
Storage Class (Storage device)	Disk	Premium	Provides a Disk resource with high-speed Disk performance (equivalent to iSCSI).
		Premium+	Provides a Disk resource with faster Disk performance than Premium (equivalent to FC).

Physical server performance

The physical configuration of one physical server that are provided are shown below.

	Small	Medium	Large

Number of physical CPU sockets	2 sockets (Number of physical CPU cores: Total of 16 cores)	4 sockets (Number of physical CPU cores: Total of 32 cores)	4 sockets (Number of physical CPU cores: Total of 32 cores)
CPU ※	32 GHz	72 GHz	96 GHz
Memory ※	128 GB	192 GB	768 GB
CPU processing capacity	Yokohama No.1: 2012 Intel Xeon Processor Kansai 1: 2012 Intel Xeon Processor		

※ About 10%-15% overhead is required for vitrtualization. So Customer can use the following amount resource approximately. As of February, 2015.

Class	Small	Medium	Large
CPU	27GHz	65GHz	80GHz
Memory	115GB	182GB	730GB

INFO

- The processing capacity of a CPU that provides 1 GHz of CPU resource is equivalent to the processing capacity when the physical processor above operates at 1 GHz.
- In Compute Resource (Dedicated Device), you can set three parameters (limit value, reserved rate, and reserved value) for the CPU resources, Memory resources, and Disk resources in order to effectively utilize the resources that can be assigned to the Virtual Machine. For details, refer to "3.2.3 Parameter Settings for Resources" (⇒P.82).

Disk resources provided by the storage device

For storage devices, you can select the storage class and plan that is appropriate for your intended use.

The storage devices and resources that can be selected when you start using the equipment are shown below.

Storage Class	Plans	Disk Resources
Premium	3 TB	3,072 GB
	6 TB	6,144 GB
	9 TB	9,216 GB
	12 TB	12,288 GB
	15 TB	15,360 GB
	18 TB	18,432 GB
	21 TB	21,504 GB
	24 TB	24,576 GB

Premium+	3 TB	3,072 GB
	6 TB	6,144 GB
	9 TB	9,216 GB
	12 TB	12,288 GB
	15 TB	15,360 GB
	18 TB	18,432 GB
	21 TB	21,504 GB
	24 TB	24,576 GB

[Reference] Target I/O performance for each storage class

	Interface	Target I/O Performance
Premium	Equivalent to iSCSI	Approx. 8,300 IOPS/24 TB, approx. 1,800 IOPS/3 TB
Premium+	Equivalent to Fiber Channel	Approx. 18,600 IOPS/24 TB, approx. 5,700 IOPS/3 TB

IOPS is one performance measure for Memory devices (such as hard Disks). It is the number of times that a read/write can be performed in one second under certain conditions. The IOPS values above are the performance values measured under the following conditions.

Measurement condition	One Virtual Machine was created in a Compute Resource Pool, benchmarking was performed multiple times, and the average value was calculated.	
Virtual machine conditions	vCPU	8
	Memory	16 GB
	Guest OS	Red Hat Enterprise Linux 6.2
Benchmark tool	fio	
Settings parameters	direct=1 (measured in unbuffered I/O) runtime=300 (measurement time is 300 seconds) size=16GB (test file size is 16 GB) readwrite=RandomReadWrite (measured in random read/writes) rwmixread=50 (read/write ratio is 50:50) blocksize=4k (block size is 4 kbyte)	

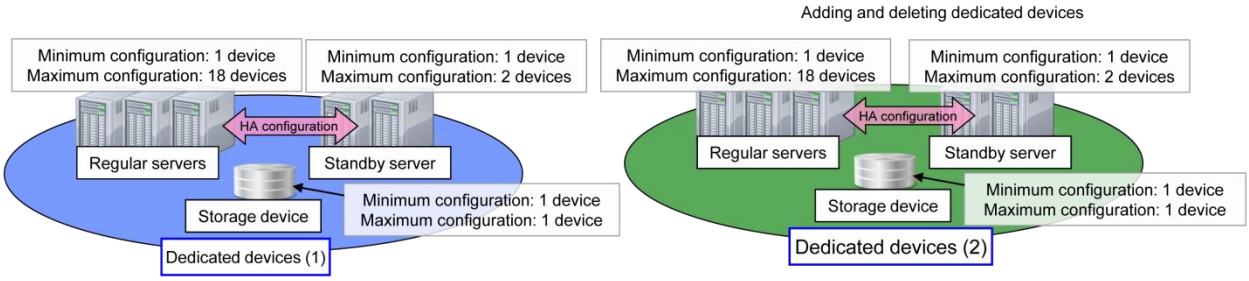
HA Cluster Feature

The same HA Cluster feature that is provided in Compute Resource is also provided in Compute Resource. For details regarding the HA Cluster feature, refer to "HA Cluster Feature" (⇒P.55).

Adding and Deleting Dedicated Devices

You can have multiple dedicated devices by reserving multiple Compute Resources (Dedicated Device).

To add or delete a dedicated device, please submit the application specified separately.



NOTE

- To delete a dedicated device, first delete all Virtual Machines that use Compute Resources on the dedicated device that you are deleting.

3.2.3 Parameter Settings for Resources

In Compute Resource (Dedicated Device), you can set three parameters (limit value, reserved rate, and reserved value) for the CPU resources, Memory resources, and Disk resources in order to effectively utilize the resources that can be assigned to the Virtual Machine.Service Order form is needed for setting.

The items marked with a "Y" are items that can be set. For example, a limit value can be set for CPU resources and Memory resources.

Item	Description	CPU	Memory	Disk
Limit value	Sets the upper limit of the resources that a Compute Resource Pool can use.	Y	Y	-
Reservation rate	Sets the percentage value of the reservation value for the limit value.	Y	Y	-
Reservation value	Sets the resource value that the Compute Resource Pool can definitely use.	Y	Y	Y

CPU Resources

You can add or reduce CPU resources within the ranges shown below.

	Lower Limit	Upper Limit	Setting Unit
Limit value	1 GHz	The resource value provided by the HA cluster	1 GHz
Reservation rate	0%	100%	1%
Reservation value	Determined based on the product of the limit value and the reserved rate.		

NOTE
- The total of the CPU resource reserved rates for all Compute Resources that belong to the same HA cluster cannot exceed the CPU resource provided by that HA cluster.

Memory Resources

You can add or reduce Memory resources within the ranges shown below.

	Lower Limit	Upper Limit	Setting Unit
Limit value	1 GB	The resource value provided by the HA cluster	1 GB
Reservation rate	20%	100%	1%
Reservation value	Determined based on the product of the limit value and the reserved rate.		

NOTE
- The total of the Memory resource reserved rates for all Compute Resources that belong to the same HA cluster cannot exceed the Memory resources provided by that HA cluster.

Disk Resources

You can add or reduce Disk resources within the ranges shown below.

	Lower Limit	Upper Limit	Setting Unit
Reservation value	50 GB	Disk resources provided by the storage device	1 GB

NOTE
- The total of the Disk resource reserved rates for all Compute Resources that belong to the same storage device cannot exceed the Disk resources provided by that storage.

INFO
- The Disk resources listed in the Customer Portal may vary slightly from the values in the table.
- Disk performance varies according to the storage class. For details, refer to "Class" (⇒P.77).

3.2.4 Assigning Resources to a Virtual Machine

Create a Virtual Machine by assigning resources in a Compute Resource Pool (CPUs/Memory/Disk) to the Virtual Machine. The amount of resources that can be assigned to a Virtual Machine is different with Customer Portal ver1.0 and Customer Portal ver2.0 . The Service Specification differences between the two portals are listed below:

vCPU

The quantities of vCPUs that can be assigned to one Virtual Machine are shown below. The configurable settings of Customer Portal ver1.0 are different from those of Customer Portal ver2.0 .

Customer Portal ver1.0

Service Menu	Compute Class	Min	Max	Step
Compute Resource (Dedicated Device)	Small	1	8	※
	Medium	1	8	※
	Large	1	8	※

※Configurable value of vCPUs are 1,2,4,6,or 8. Odd number vCPUs cannot be configured on Customer Portal ver1.0 .

Customer Portal ver2.0

Service Menu	Compute Class	Min	Max	Step
Compute Resource (Dedicated Device)	Small	1	16	1
	Medium	1	32	1
	Large	1	32	1

Memory

You can add or reduce the Memory capacity that is assigned to one Virtual Machine within the ranges shown below. The configurable settings of Customer Portal ver1.0 are different from those of Customer Portal ver2.0 .

Customer Portal ver1.0

Service Menu	Compute Class	Min	Max	Step
Compute Resource (Dedicated Device)	Small	1	8	1
	Medium	1	8	1
	Large	1	8	1

Customer Portal ver2.0

Service Menu	Compute Class	Min	Max	Step
Compute Resource (Dedicated Device)	Small	1	96	1
	Medium	1	128	1
	Large	1	512	1

Disk

You can add or reduce the Disk capacity and the number of data Disks connected to one Virtual Machine within the ranges shown below. The configurable settings of Customer Portal ver1.0 are different from those of Customer Portal ver2.0 .

Customer Portal ver1.0

	Lower Limit	Upper Limit	Setting Unit
Number of data Disks	0	6	1
Disk capacity	1 GB	2,000 GB	1 GB

Customer Portal ver2.0

	Lower Limit	Upper Limit	Setting Unit
Number of data Disks	0	59	1
Disk capacity	1 GB	2,047 GB	1 GB
	1 MB	2,097,151 MB	1 MB

3.2.5 Important Points

- You cannot "change the storage class (Premium or Premium+)" or "add one or more storage devices." You therefore need to consider your future storage usage plan when selecting a storage class at the time of your application.
- You can "change your storage device plan (add a Disk resource). However, you cannot change to a plan that decreases the Disk resource value.
- If you "change your storage device plan," the date that the change application takes effect becomes the new starting date for calculating the minimum usage period for your contract.

- Compute Class (Small, Medium, Large) cannot create the same cluster.The same class of the physical server can be added within the limit range.
- Compute Class (Small, Large) is only provided in Japan DC, Compute Class (Medium) is provided in US,UK,SG. Please refer to “Service Provided in each Data Center”.

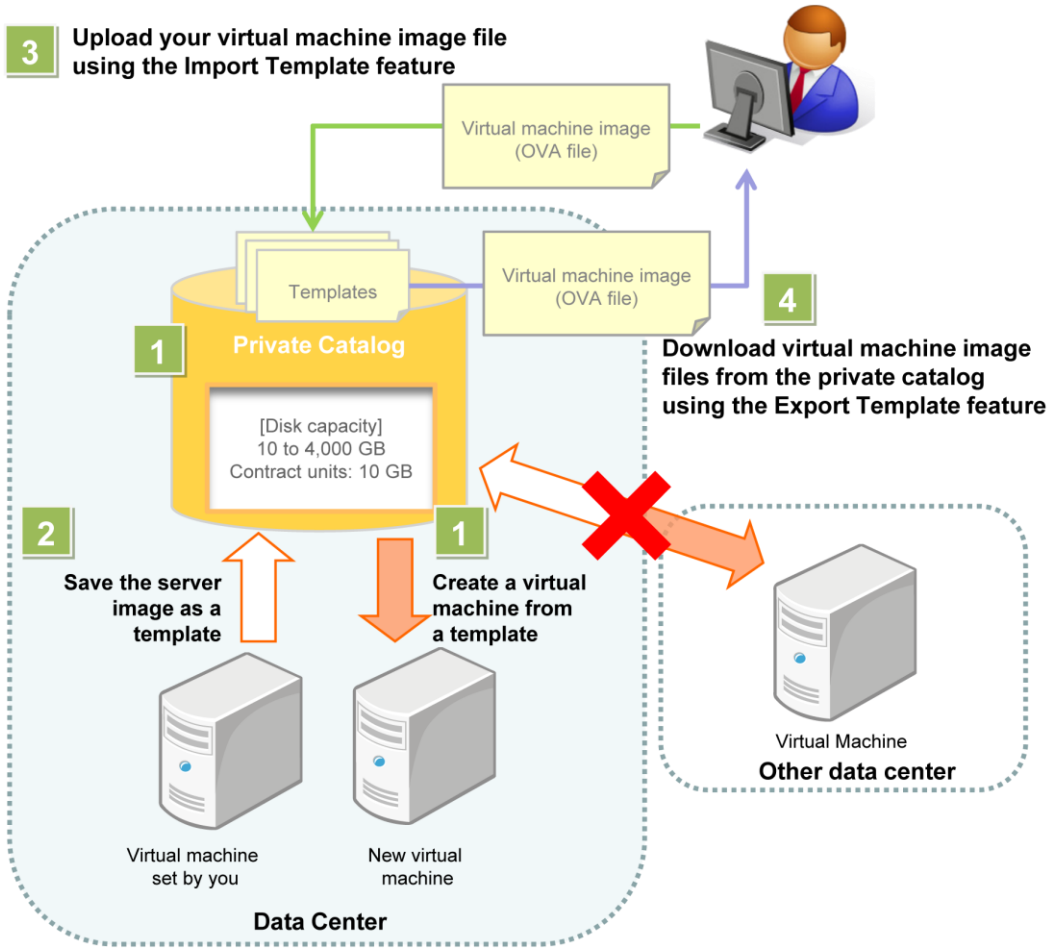
3.3 Private Catalog

Private Catalog is a service that provides Disks for storing templates of Virtual Machines that you have created. You can create new Virtual Machines from the templates saved in Private Catalog.

3.3.1 Available Features

You can use the following features in Private Catalog.

	Feature	Overview
1	Provision of a Disk for saving template catalogs	A feature that provides a Disk region for saving Virtual Machine templates and adds or reduces the capacity. You can create new Virtual Machines from the templates saved in this Disk region.
2	Create Template feature	A feature that converts a created Virtual Machine into a template. You can also delete created templates.
3	Import Template feature	A feature for importing Virtual Machine images created on a local server to Private Catalog.
4	Export Template feature	A feature for exporting templates stored in Private Catalog to a local server.



NOTE
- Private Catalog can only be used in the same Data Center as the Compute Resource Pool. It cannot be used across different Data Centers.

INFO
- The Private Catalog Disk region is provided by using the Disk resources of storage devices shared by multiple users. Disk resources are provided as user-specific Private Catalogs and therefore cannot be accessed by other users.

3.3.2 Provision of a Disk for Saving Template Catalogs

You can use the Customer Portal to add or reduce the capacity of the Private Catalog Disk region within the ranges shown below.

Item	Lower Limit	Upper Limit	Setting Unit
Disk Resources	10 GB	4,000 GB	10 GB

NOTE
- Guest OS license usage fees are incurred if you create a template of a Virtual Machine that contains an OS license provided by Compute Resource, and then create a Virtual Machine based on the template. For details regarding the applicable types of Guest OSes, refer to "3.4 OS License" (⇒P.92).
- If the Virtual Machine is over 4,000GB for total disk capacity + memory resource (different for each Compute Class), the template cannot be created.

INFO
- You can also delete all Private Catalog Disk regions.

3.3.3 Create Template Feature

You can convert a created Virtual Machine and save it as a template in a Private Catalog. You can also delete stored templates.

When creating a template, confirm that the following requirements have been met.

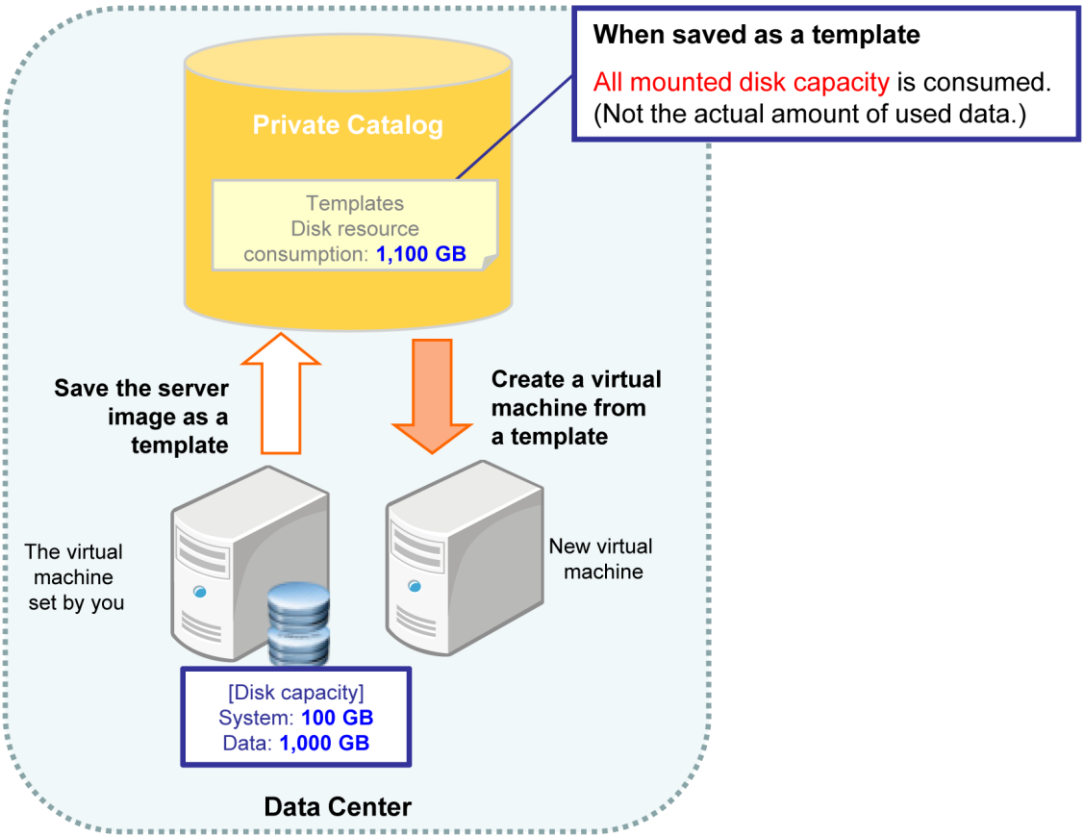
- The Virtual Machine is powered off
- The Private Catalog Disk region has more available space than the total value of the Disk capacity and Memory capacity of the Virtual Machine

INFO
- The Virtual Machine is not deleted by creating and deleting templates. The configuration of the root Disk and data Disks for the Virtual Machine and the data are preserved.

Understanding the Consumption of Private Catalog Disk Resources

When creating a template, the following capacity is consumed from the Private Catalog Disk resources.

- Total value of all of the Disk capacity mounted in the Virtual Machine



INFO

- The Private Catalog Disk resources consumed by templates are only the total value of the Disk capacity of the Virtual Machine that created the Virtual Machine image. It does not include the Memory capacity.

3.3.4 Import Template Feature

You can import Virtual Machine images created on a local server to Private Catalog.

If you upload a Virtual Machine image file from the Customer Portal using a web browser, the Virtual Machine image file is converted into a template and saved in the Private Catalog.

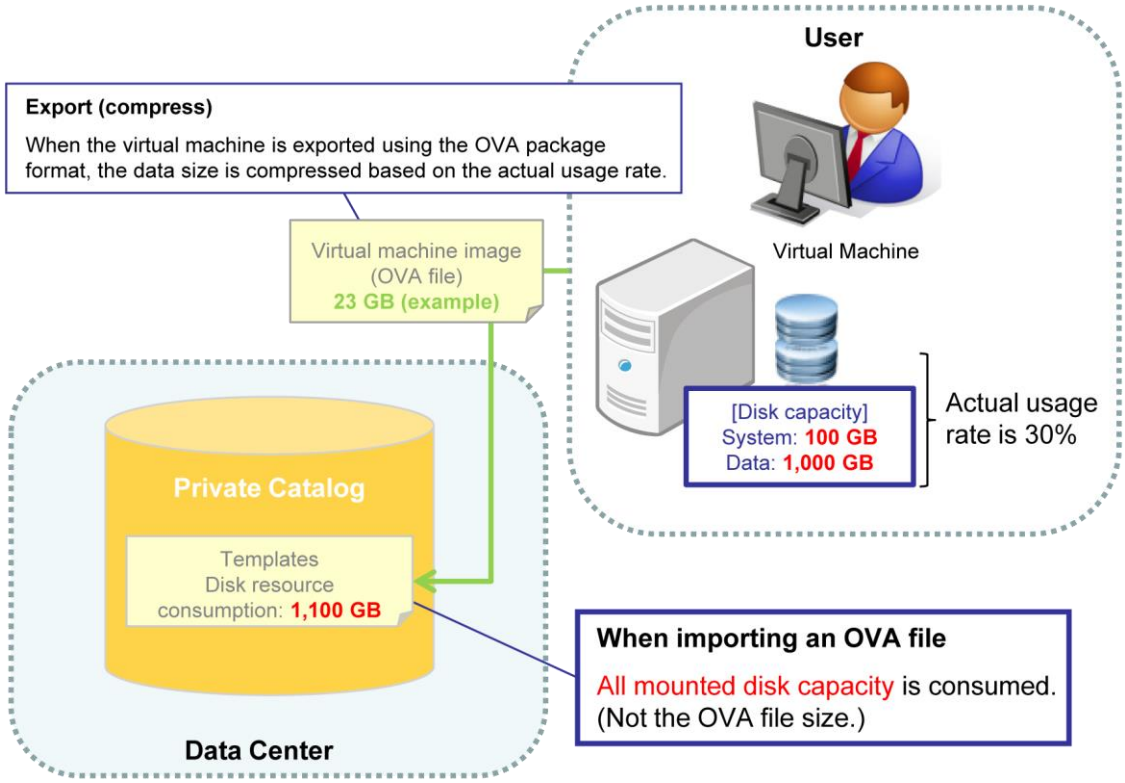
NOTE

- To import a Virtual Machine image, you will require more available space in the Private Catalog Disk region than the total of the Disk capacity and Memory capacity of the Virtual Machine image that is being imported (not the file size of the actual OVA file).
- For the conditions for Virtual Machine images that can be imported, refer to the "User's Guide For the Virtual Machine Image Import/Export Feature."
- You are responsible for appropriately managing licenses for software such as Guest OSes and applications included in the imported Virtual Machine image. For example, please check with the vendor of your Guest OS or application to confirm that the license can be used in Compute Resource, prior to use.
- For the Guest OS to import and use a Virtual Machine image of Windows Server, you will need to switch the OS license under local options.

Understanding the Consumption of Private Catalog Disk Resources

When importing a template, the following capacity is consumed from the Private Catalog Disk resources.

- Total value of all of the Disk capacity mounted in the Virtual Machine



INFO

- The Private Catalog Disk resources consumed by templates are only the total value of the Disk capacity of the Virtual Machine that created the Virtual Machine image. It does not include the Memory capacity.

3.3.5 Export Template Feature

You can convert a Private Catalog template to a Virtual Machine image and export it from the Customer Portal to your own environment using a Web browser.

NOTE

- If NTT Communications owns the licenses for software included in the exported Virtual Machine image, such as the Guest OS and applications, the continued use of those licenses on your local computer is a license violation and is therefore not permitted. In this situation, you are responsible for appropriately managing licenses by replacing the licenses for such software with licenses that you own.

INFO

- Download sessions established while logged in to the Customer Portal can be continued after logging out of the Customer Portal. However, the download session may be terminated after downloading continuously for more than 48 hours.
- A template is not deleted even if you export it.

3.3.6 Important Points

Important Points regarding the Windows Server Guest OS

When creating a Virtual Machine from a template that uses Windows Server as the Guest OS, Sysprep will automatically run the first time that you start the Virtual Machine. Sysprep is a tool that configures Windows OS system settings in advance.

NOTE

- Microsoft product specifications and license terms allow you to run Sysprep up to the limit listed below.. If you exceed this limit, you may not be able to use the Virtual Machine.

  Windows Server 2012 R2: 1000 times

  Windows Server 2012: 1000 times

  Windows Server 2008 R2: 3 times

  ※Once the virtual machine is created from the template, you will be using up the limited times for Sysprep running.

Important Points regarding Guest OS Settings

When changing the Guest OS network settings, do not disable a vNIC that has been recognized in the Customer Portal, even if you are not using that vNIC. Creating a Virtual Machine from a template in which vNIC is disabled in the Guest OS may result in errors.

Important Points regarding Serves Segment deletion

Server Segment cannot be deleted as long as the templete exist on Private Catalog, when Virtual Machine which vNIC connecting the Server Segment is converted. When

there is a schedule which deletes Server Segment, please convert Virtual Machine after removing vNIC from the Server Segment in advance.

3.4 OS License

OS License is a service that provides rights to use an OS license for the Windows Server operating system or a Red Hat Enterprise Linux subscription on Virtual Machines created in Compute Resource.

INFO
- NTT Communications provides OS licenses as its own service, based on a contract signed under Microsoft's SPLA license agreement, and subscriptions as its own service, based on an agreement with Red Hat.

3.4.1 Available Features

You can use the following features in OS License.

Feature	Overview
Provision of an OS license	A feature for using an OS license to run Windows or Linux on a Virtual Machine in Compute Resource.
Provision of a Public Catalog	A feature that uses a template of the OS-installed Virtual Machine to provide the above license.

3.4.2 Provision of an OS License

The OS licenses and subscriptions provided in OS License are shown below. One license is provided for one Virtual Machine.

Microsoft OS license	Windows Server 2008 R2 Enterprise Japanese/English Windows Server 2012 Standard Japanes/English Windows Server 2012 R2 Standard Japanes/English	64bit version
Red Hat subscription	Red Hat Enterprise Linux Server 5.8/6.2 Japanese/English keyboard layout	64bit version

INFO
- When you use OS License, you can use the "software access" and "software maintenance" features from the Red Hat Enterprise Linux software subscription. Please follow the instructions from NTT Communications regarding the procedure and access method for using these features.

3.4.3 Provision of a Public Catalog

You can use a template for creating a Virtual Machine for which a Microsoft OS license and Red Hat subscription have been provided.

You can use templates from the Customer Portal when creating a Virtual Machine in Compute Resource or Compute Resource (Dedicated Device).

NOTE

- A Microsoft OS license and Red Hat subscription are only provided for a Virtual Machine created using the provided template (called a "Virtual Machine created with OS License" below).

INFO

- When you use the template to create a Virtual Machine, you can use the OS-installed Virtual Machine immediately.
- Templates exist for each Data Center and are stored in the Public Catalog, which can be accessed by all users of that Data Center.

3.4.4 Important Points

- OS License does not include monitoring and operating services for the OS.
- NTT Communications does not provide support (investigations, assistance, or advice) for requests from users regarding troubleshooting procedures for errors relating to installation, setup, or basic functionality that you encounter for licensed products that you are using in OS License.
- When using programs provided in OS License, it is assumed that you agree with the Services Provider Use Rights (SPUR) when using Microsoft products, or the Red Hat Enterprise Agreement when using Red Hat products. For details, refer to the following URLs.

  - Microsoft Services Provider Use Rights (SPUR)

    http://www.microsoftvolumelicensing.com/userights/DocumentSearch.aspx?Mode=3&DocumentTypeId=2

    ※ Refer to the latest version of the Services Provider Use Rights (Worldwide) (Japanese).
  - Red Hat Enterprise Agreement

    http://www.jp.redhat.com/licenses/Enterprise_Agr_Japan.pdf

- Information required for installation, such as an activation key or subscription number, cannot be disclosed directly to users in writing or by any other means.

Windows Restrictions

- You can install the following Microsoft products on a Virtual Machine created with OS License.
  - Products that you have permission to use on a shared server
- When using Complete Memory Dump, you need at least "the Memory assigned to the Virtual Machine + 300 MB" of available space on the drive on which the dump files are created.
- Regarding the License Certification for Windows Server 2012 Standard and Windows Server 2012 R2 Standard.
  - Customer needs to adjust the time by using NTP server.License will not be activated if there is a lag between the Server time and the actual time.
  - The default gateway of the Virtual Machine needs to be set on the vFirewall.

    If customer will set the default gateway on other than vFirewall, they would have to set by static routing. Global IP Address is being used as a host for license activation, but the transmission itself is closed with NTT Com platform and it will never go out to the Internet. For more details on the static routing, please contact the techinical help desk individually.

Red Hat Enterprise Linux Restrictions

- Virtual machines created with OS License must be registered in the Red Hat network, and all registrations must be up to date.
- OS license does not provide users with RHN login ID information for logging in to the Red Hat Customer Portal (formerly known as the Red Hat Network).
- If you want to install optional software that includes a Red Hat Enterprise Linux subscription, please use the yum interface for installation. NTT Communications can also install the software for a fee.
-

Prohibited Acts

The acts listed below violate the agreement between the user and Microsoft or the Enterprise Agreement with Red Hat, or are considered incorrect usage as stipulated in the NTT Communications Service Feature Overview or Conditions For Providing Services. Users engaged in such acts may be subject to penalties imposed by NTT Communications such as suspension of service, or incorrect usage penalties imposed by Microsoft.

The following acts are specific examples. The acts that may be subject to penalties are not limited to the acts below.

- Using licensed products or subscription products provided through OS License outside of the cloud environment specified by NTT Communications.
- Using the Customer Portal features to create and save another template of the Virtual Machine image, using the export feature to store the template outside of the NTT Communications cloud environment, creating a new Virtual Machine based on

that file, and running licensed products or subscription products that have been provided by NTT Communications.

- Duplicating and using the software without notifying NTT Communications.
- Using OS License to duplicate the image of the Virtual Machine that you are running and then running it as another Virtual Machine without changing the registration information and without notifying NTT Communications.

3.5 Database License (MS SQL)

Database License (MS SQL) is a service that provides a Microsoft license for Microsoft SQL Server on Virtual Machines created in Compute Resource.

INFO

- In Database License (MS SQL), NTT Communications provides database licenses as its own service, based on a contract signed under Microsoft's SPLA license agreement.

3.5.1 Available Features

You can use the following features in Database License (MS SQL).

Feature	Overview
Provision of a Database License	A feature for using a Database License to run Microsoft SQL Server on a Virtual Machine in Compute Resource.
Provision of a Public Catalog	A feature that uses a template of the Microsoft SQL Server-installed Virtual Machine to provide the above license.

3.5.2 Provision of a Database License

The following licenses are provided by Database License (MS SQL).

OS	Database
Windows Server 2008 R2 Enterprise	SQL Server 2008 R2 Standard (64bit) –Japanese/English SQL Server 2012 Standard (64bit) – Japanese/English
Windows Server 2012 Standard	SQL Server 2012 Standard SP2 (64bit) – Japanese/English SQL Server 2014 Standard (64bit) – Japanese/English

The Database License that are provided with Windows Server 2012 Standard is currently available in Japan Datacenters. The service will be available in other Datacenters

Provision of a Public Catalog

You can use the templates provided by Database License to create a Virtual Machine. You can use templates from the Customer Portal when creating a Virtual Machine in Compute Resource or Compute Resource (Dedicated Device).

NOTE

- A Database license is only provided for a Virtual Machine created using the provided template (called a "Virtual Machine created with Database License (MS SQL)" below).
- One Database License and one OS License are provided as a set for one

Virtual Machine created using Database License (MS SQL).

For details regarding the conditions for providing an OS license, refer to "3.4 OS License" (⇒P.92).

- SQL Server is installed the first time that you start a Virtual Machine created with Database License (MS SQL). It will therefore take approximately two hours before the login screen is displayed for the first time. Do not perform operations that suspend processing (power off, reset, shutdown, suspend, or restart the Virtual Machine) while you are waiting for the login screen to appear.

INFO

- Templates exist for each Data Center and are stored in the Public Catalog, which can be accessed by all users of that Data Center.

3.5.3 Important Points

- You cannot save a Virtual Machine created with Database License (MS SQL) to the Private Catalog in Data Centers where the service for creating a Virtual Machine from a Private Catalog is not provided.
- The Disk capacity required to SQL Server is shown below.

SQL Server Type	Required Disk Capacity
SQL Server 2008 R2 Standard SP2 Japanese 64bit version	Approximately 7 GB
SQL Server 2012 Standard SP1 Japanese 64bit version	Approximately 13 GB
SQL Server 2012 Standard SP2 Japanese 64bit version	Approximately 11GB
SQL Server 2014 Standard Japanese 64bit version	Approximately 6GB
SQL Server 2008 R2 Standard SP2 English 64bit version	Approximately 7 GB
SQL Server 2012 Standard SP1 English 64bit version	Approximately 13 GB
SQL Server 2012 Standard SP2 English 64bit version	Approximately 11GB
SQL Sevrver 2014 Standard English 64bit version	Approximately 6GB

- You can use between one and four vCPUs with SQL Server Standard Edition. Please do not set more than five vCPUs on Customer Portal ver2.0 . If the customer has set more than five vCPUs, please contact NTTCom individually. You cannot change the SQL Server type for a Virtual Machine created with Database License (MS SQL).
- If you reinstall SQL Server, create the Virtual Machine again from the template.
- The template specifications may change.

Prohibited Acts

The acts listed below violate the agreement between the user and Microsoft, or are considered incorrect usage of NTT Communications services. Users engaged in such

acts may be subject to penalties imposed by NTT Communications such as suspension of service, or incorrect usage penalties imposed by Microsoft.

The following acts are specific examples. The acts that may be subject to penalties are not limited to the acts below.

- Using licensed products provided through Database License (MS SQL) outside of the cloud environment specified by NTT Communications.
- Using the Customer Portal features to create and save another template of the Virtual Machine image, using the export feature to store the template outside of the NTT Communications cloud environment, creating a new Virtual Machine based on that file, and running licensed products that have been provided by NTT Communications.
- Duplicating and using the software without notifying NTT Communications.
- Using Database License (MS SQL) to duplicate the image of the Virtual Machine that you are running and then running it as another Virtual Machine without notifying NTT Communications.

3.5.4 Initial State of Microsoft SQL Server

For SQL Server 2008 R2 Standard Japanese

Item	Settings Information	Remark
Feature selection		
Instance feature		
Database engine service	Selected	
SQL Server replication	Selected	
Full-text search	Selected	
Analysis Services	Selected	
Reporting Services	Selected	
Shared features		
Business Intelligence Development Studio	Selected	
Client tool connection	Selected	
Integration Services	Selected	
Client tools backward compatibility	Selected	
Client Tools SDK	Selected	
SQL Server online book	Selected	
Management tools - basic	Selected	
Management tools - complete	Selected	
SQL Client Connection SDK	Selected	
Microsoft Sync Framework	Selected	
Shared feature directory	C:\Program Files\Microsoft SQL Server\	
Shared feature directory (x86)	C:\Program Files (x86)\Microsoft SQL Server\	
Instance configuration		
Instance	Default instance	
Instance ID	MSSQLSERVER	
Instance root directory	C:\Program Files\Microsoft SQL Server\	
Server configuration		
Service account		
Service: SQL Server Agent		
Account name	NT AUTHORITY\NETWORK SERVICE	
Startup type	Manual	
Service: SQL Server Database Engine		
Account name	NT AUTHORITY\NETWORK SERVICE	
Startup type	Automatic	
Service: SQL Server Analysis Services		
Account name	NT AUTHORITY\NETWORK SERVICE	
Startup type	Automatic	
Service: SQL Server Reporting Services		
Account name	NT AUTHORITY\NETWORK SERVICE	
Startup type	Automatic	
Service: SQL Server Integration Services		
Account name	NT AUTHORITY\NetworkService	
Startup type	Automatic	
Service: SQL Full-text filter Daemon Launcher		
Account name	NT AUTHORITY\LOCAL SERVICE	
Startup type	Manual	
Service: SQL Server Browser		
Account name	NT AUTHORITY\LOCAL SERVICE	
Startup type	Disabled	
Collation sequence		
Database engine		
Collation sequence	Japanese_CI_AS	
Analysis Services		
Collation sequence	Japanese_CI_AS	

Database engine configuration			
	Account provisioning		
	Authentication mode	Windows authentication mode	
	Specify SQL Server administrators	Administrator	
	Data directory		
	Data root directory	C:\Program Files\Microsoft SQL Server\	
	User database directory	C:\Program Files\Microsoft SQL Server\ MSSQL10_50.MSSQLSERVER\MSSQL\Data	
	User database log directory	C:\Program Files\Microsoft SQL Server\ MSSQL10_50.MSSQLSERVER\MSSQL\Data	
	Temp DB directory	C:\Program Files\Microsoft SQL Server\ MSSQL10_50.MSSQLSERVER\MSSQL\Data	
	Temp DB log directory	C:\Program Files\Microsoft SQL Server\ MSSQL10_50.MSSQLSERVER\MSSQL\Data	
	Backup directory	C:\Program Files\Microsoft SQL Server\ MSSQL10_50.MSSQLSERVER\MSSQL\Backup	
	FILESTREAM		
	Enable FILESTREAM for Transact-SQL access	Disabled	
Analysis Services configuration			
	Account provisioning		
	Specify SQL Server administrators	Administrator	
	Data directory		
	Data directory	C:\Program Files\Microsoft SQL Server\ MSAS10_50.MSSQLSERVER\OLAP\Data	
	Log file directory	C:\Program Files\Microsoft SQL Server\ MSAS10_50.MSSQLSERVER\OLAP\Log	
	Temporary directory	C:\Program Files\Microsoft SQL Server\ MSAS10_50.MSSQLSERVER\OLAP\Temp	
	Backup directory	C:\Program Files\Microsoft SQL Server\ MSAS10_50.MSSQLSERVER\OLAP\Backup	
Reporting Services configuration			
	Reporting Services configuration	Install but do not configure the report server.	

For SQL Server 2012 Standard Japanese

Item	Settings Information	Remark
Feature selection		
Instance feature		
Database engine service	Selected	
SQL Server replication	Selected	
Full-text and semantic extractions for search	Selected	
Data Quality Services	Selected	
Analysis Services	Selected	
Reporting Services - Native	Selected	
Shared features		
Reporting Services - SharePoint	Selected	
Reporting Services add-in for SharePoint	Selected	
Data Quality Client	Selected	
SQL Server Data Tools	Selected	
Client tools conection	Selected	
Integration Services	Selected	
Client tools backward compatibility	Selected	
Client Tools SDK	Selected	
Document component	Selected	
Management tools - basic	Selected	
Management tools - complete	Selected	
Distributed replay controller	Selected	
Distributed replay client	Selected	
SQL Client Connection SDK	Selected	
Shared feature directory	C:\Program Files\Microsoft SQL Server\	
Shared feature directory (x86)	C:\Program Files (x86)\Microsoft SQL	
Instance configuration		
Instance	Default instance	
Instance ID	MSSQLSERVER	
Instance root directory	C:\Program Files\Microsoft SQL Server\	
Server configuration		
Service account		
Service: SQL Server agent		
Account name	NT Service\SQLSERVERAGENT	
Startup type	Manual	
Service: SQL Server database engine		
Account name	NT Service\MSSQLSERVER	
Startup type	Automatic	
Service: SQL Server Analysis Services		
Account name	NT Service\MSSQLServerOLAPService	
Startup type	Automatic	
Service: SQL Server Reporting Services		
Account name	NT Service\ReportServer	
Startup type	Automatic	
Service: SQL Server Integration Services 11.0		
Account name	NT Service\MsDtsServer110	
Startup type	Automatic	
Service: SQL Server Distributed Replay Client		
Account name	NT Service\SQL Server Distributed Replay Client	
Startup type	Manual	
Service: SQL Server Distributed Replay Controller		
Account name	NT Service\SQL Server Distributed Replay Controller	
Startup type	Manual	
Service: SQL full-text filter daemon launcher		
Account name	NT Service\MSSQLFDLauncher	
Startup type	Manual	
Service: SQL Server Browser		
Account name	NT AUTHORITY\LOCAL SERVICE	
Startup type	Disabled	

	Collation sequence		
	Database engine		
	Collation sequence	Japanese_CI_AS	
	Analysis Services		
	Collation sequence	Japanese_CI_AS	
Database engine configuration			
	Account provisioning		
	Authentication mode	Windows authentication mode	
	Specify SQL Server administrators	Administrator	
	Data directory		
	Data root directory	C:\Program Files\Microsoft SQL Server\	
	User database directory	C:\Program Files\Microsoft SQL Server\ MSSQL11.MSSQLSERVER\MSSQL\Data	
	User database log directory	C:\Program Files\Microsoft SQL Server\ MSSQL11.MSSQLSERVER\MSSQL\Data	
	Temp DB directory	C:\Program Files\Microsoft SQL Server\ MSSQL11.MSSQLSERVER\MSSQL\Data	
	Temp DB log directory	C:\Program Files\Microsoft SQL Server\ MSSQL11.MSSQLSERVER\MSSQL\Data	
	Backup directory	C:\Program Files\Microsoft SQL Server\ MSSQL11.MSSQLSERVER\MSSQL\Backup	
	FILESTREAM		
	Enable FILESTREAM for Transact-SQL access	Disabled	
Analysis Services configuration			
	Server configuration		
	Server mode	Multidimensional and data mining mode	
	Analysis Services administrator	Administrator	
	Data directory		
	Data directory	C:\Program Files\Microsoft SQL Server\ MSAS11.MSSQLSERVER\OLAP\Data	
	Log file directory	C:\Program Files\Microsoft SQL Server\ MSAS11.MSSQLSERVER\OLAP\Log	
	Temporary directory	C:\Program Files\Microsoft SQL Server\ MSAS11.MSSQLSERVER\OLAP\Temp	
	Backup directory	C:\Program Files\Microsoft SQL Server\ MSAS11.MSSQLSERVER\OLAP\Backup	
Reporting Services configuration			
	Reporting Services native mode	Install only.	
	Reporting Services SharePoint Integrated mode	Install only.	
Distributed replay controller			
	Authorized user	Administrator	
Distributed replay client			
	Controller name		Blank
	Working directory	C:\Program Files (x86)\Microsoft SQL Server\DReplayClient\WorkingDir\	
	Results directory	C:\Program Files (x86)\Microsoft SQL Server\DReplayClient\ResultDir\	

For SQL Server 2008 R2 Standard English

Item	Settings Information	Remark
Feature Selection		
Instance Features		
Database Engine Services	Selected	
SQL Server Replication	Selected	
Full-Text Search	Selected	
Analysis Services	Selected	
Reporting Services	Selected	
Shared Features		
Business Intelligence Development Studio	Selected	
Client Tools Connectivity	Selected	
Integration Services	Selected	
Client Tools Backwards Compatibility	Selected	
Client Tools SDK	Selected	
SQL Server Books Online	Selected	
Management Tools-Basic	Selected	
Management Tools - Complete	Selected	
SQL Client Connectivity SDK	Selected	
Microsoft Sync Framework	Selected	
Shared Feature directory	C:\Program Files\Microsoft SQL Server\	
Shared Feature directory (x86)	C:\Program Files (x86)\Microsoft SQL	
Instance Configuration		
Instance	Default instance	
Instance ID	MSSQLSERVER	
Instance root directory	C:\Program Files\Microsoft SQL Server\	
Server Configuration		
Service Accounts		
Service:SQL Server Agent		
Account name	NT AUTHORITY\NETWORK SERVICE	
Startup type	Manual	
Service:SQL Server Database Engine		
Account Name	NT AUTHORITY\NETWORK SERVICE	
Startup Type	Automatic	
Service:SQL Server Analysis Services		
Account Name	NT AUTHORITY\NETWORK SERVICE	
Startup Type	Automatic	
Service:SQL Server Reporting Services		
Account Name	NT AUTHORITY\NETWORK SERVICE	
Startup Type	Automatic	
Service:SQL Server Integration Services 10.0		
Account Name	NT AUTHORITY\NetworkService	
Startup Type	Automatic	
Service:SQL Full-text filter Daemon Launcher		
Account Name	NT AUTHORITY\LOCAL SERVICE	
Startup Type	Manual	
Service:SQL Server Browser		
Account Name	NT AUTHORITY\LOCAL SERVICE	
Startup Type	Disabled	
Collation		
Database Engine		
collation	SQL_Latin1_General_CP1_CI_AS	
Analysis Services		
collation	Latin1_General_CI_AS	

Database Engine Configuration			
	Account Provisioning		
	Authentication Mode	Windows authentication mode	
	Spacify SQL Server administrators	Administrator	
	Data Directories		
	Data root directory	C:\Program Files\Microsoft SQL Server\	
	User database directory	C:\Program Files\Microsoft SQL Server\ MSSQL10_50.MSSQLSERVER\MSSQL\Data	
	User databaselog directory	C:\Program Files\Microsoft SQL Server\ MSSQL10_50.MSSQLSERVER\MSSQL\Data	
	Temp DB directory	C:\Program Files\Microsoft SQL Server\ MSSQL10_50.MSSQLSERVER\MSSQL\Data	
	Temp DB log directory	C:\Program Files\Microsoft SQL Server\ MSSQL10_50.MSSQLSERVER\MSSQL\Data	
	Backup directory	C:\Program Files\Microsoft SQL Server\ MSSQL10_50.MSSQLSERVER\MSSQL\Backup	
	FILESTREAM		
	Enable FILESTREAM for Transact-SQL access	Disabled	
Analysis Services Configuration			
	Account Provisioning		
	Spacify which users have administrative permissions for An	Administrator	
	Data Directories		
	Data directory	C:\Program Files\Microsoft SQL Server\ MSAS10_50.MSSQLSERVER\OLAP\Data	
	Log file directory	C:\Program Files\Microsoft SQL Server\ MSAS10_50.MSSQLSERVER\OLAP\Log	
	Temp directory	C:\Program Files\Microsoft SQL Server\ MSAS10_50.MSSQLSERVER\OLAP\Temp	
	Backup directory	C:\Program Files\Microsoft SQL Server\ MSAS10_50.MSSQLSERVER\OLAP\Backup	
Reporting Services Configuration			
	Reporting Services Configuration	Install but do not configure the report server.	

For SQL Server 2012 Standard English

Item	Settings Information	Remark
Feature Selection		
Instance Features		
Database Engine Services	Selected	
SQL Server Replication	Selected	
Full-Text and Semantic Extractions for Search	Selected	
Data Quality Services	Selected	
Analysis Services	Selected	
Reporting Services - Native	Selected	
Shared Features		
Reporting Services - SharePoint	Selected	
Reporting Services Add-in for SharePoint Products	Selected	
Data Quality Client	Selected	
SQL Server Data Tools	Selected	
Client Tools Connectivity	Selected	
Integration Services	Selected	
Client Tools Backwards Compatibility	Selected	
Client Tools SDK	Selected	
Documentation Components	Selected	
Management Tools - Basic	Selected	
Management Tools - Complete	Selected	
Distributed Replay Controller	Selected	
Distributed Replay Client	Selected	
SQL Client Connectivity SDK	Selected	
Shared Feature directory	C:\Program Files\Microsoft SQL Server\	
Shared Feature directory (x86)	C:\Program Files (x86)\Microsoft SQL	
Instance Configuration		
Instance	Default instance	
Instance ID	MSSQLSERVER	
Instance root directory	C:\Program Files\Microsoft SQL Server\	
Server Configuration		
Service Accounts		
Service:SQL Server Agent		
Account Name	NT Service\SQLSERVERAGENT	
Startup Type	Manual	
Service:SQL Server Database Engine		
Account Name	NT Service\MSSQLSERVER	
Startup Type	Automatic	
Service:SQL Server Analysis Services		
Account Name	NT Service\MSSQLServerOLAPService	
Startup Type	Automatic	
Service:SQL Server Reporting Services		
Account Name	NT Service\ReportServer	
Startup Type	Automatic	
Service:SQL Server Integration Services 11.0		
Account Name	NT Service\MsDtsServer110	
Startup Type	Automatic	
Service:SQL Server Distributed Replay Client		
Account Name	NT Service\SQL Server Distributed Replay Client	
Startup Type	Manual	
Service:SQL Server Distributed Replay Controller		
Account Name	NT Service\SQL Server Distributed Replay Controller	
Startup Type	Manual	
Service:SQL Full-text Filter Daemon Launcher		
Account Name	NT Service\MSSQLFDLauncher	
Startup Type	Manual	
Service:SQL Server Browser		
Account Name	NT AUTHORITY\LOCAL SERVICE	
Startup Type	Disabled	
Collation		
Database Engine		
collation	SQL_Latin1_General_CP1_CI_AS	
Analysis Services		
collation	Latin1_General_CI_AS	

Database Engine Configuration			
	Server Configuration		
	Authentication Mode	Windows authentication mode	
	Spacify SQL Server administrators	Administrator	
	Data Directories		
	Data root directory	C:\Program Files\Microsoft SQL Server\	
	User database directory	C:\Program Files\Microsoft SQL Server\ MSSQL11.MSSQLSERVER\MSSQL\Data	
	User databaselog directory	C:\Program Files\Microsoft SQL Server\ MSSQL11.MSSQLSERVER\MSSQL\Data	
	Temp DB directory	C:\Program Files\Microsoft SQL Server\ MSSQL11.MSSQLSERVER\MSSQL\Data	
	Temp DB log directory	C:\Program Files\Microsoft SQL Server\ MSSQL11.MSSQLSERVER\MSSQL\Data	
	Backup directory	C:\Program Files\Microsoft SQL Server\ MSSQL11.MSSQLSERVER\MSSQL\Backup	
	FILESTREAM		
	Enable FILESTREAM for Transact-SQL access	Disabled	
Analysis Services Configuration			
	Server Configuration		
	Server Mode	Multidimensional and data mining mode	
	Spacify which users have administrative permissions for Analysis Services	Administrator	
	Data Directories		
	Data directory	C:\Program Files\Microsoft SQL Server\ MSAS11.MSSQLSERVER\OLAP\Data	
	Log file directory	C:\Program Files\Microsoft SQL Server\ MSAS11.MSSQLSERVER\OLAP\Log	
	Temp directory	C:\Program Files\Microsoft SQL Server\ MSAS11.MSSQLSERVER\OLAP\Temp	
	Backup directory	C:\Program Files\Microsoft SQL Server\ MSAS11.MSSQLSERVER\OLAP\Backup	
Reporting Services Configuration			
	Reporting Services Native Mode	Install only.	
	Reporting Services SharePoint Integrated Mode	Install only.	
Distributed Replay Controller			
	Spacify which users have permissions for the Distributed Replay Controller service	Administrator	
Distributed Replay Client			
	Controller Name		Blank
	Working Directory	C:\Program Files (x86)\Microsoft SQL Server\DReplayClient\WorkingDir\	
	Result Directory	C:\Program Files (x86)\Microsoft SQL Server\DReplayClient\ResultDir\	

For SQL Server 2014 Standard Japanese

Item	Settings	Remark
Feature Selection		
Instance Feature		
Database Engine Service	Selected	
SQL Server replication	Selected	
Full-text search and Symantec search	Selected	
Data Quality Services	Selected	
Analysis Services	Selected	
Reporting Services - Native	Selected	
Shared Features		
Reporting Services - SharePoint	Selected	
Reporting Services Add-in for SharePoint Products	Selected	
Data Quality Client	Selected	
Client Tools Connectivity	Selected	
Integration Services	Selected	
Client Tools Backwards Compatibility	Selected	
Client Tools SDK	Selected	
Documentation Components	Selected	
Management Tools - Basic	Selected	
Management Tools - Complete	Selected	
Distributed Replay Controller	Selected	
Distributed Replay Client	Selected	
SQL Client Connectivity SDK	Selected	
Instance root directory	C:¥Program Files¥Microsoft SQL Server¥	
Shared Feature directory	C:¥Program Files¥Microsoft SQL Server¥	
Shared Feature directory (x86)	C:¥Program Files (x86)¥Microsoft SQL Server¥	
Instance Configuration		
Instance	Default instance	
Instance ID	MSSQLSERVER	
Server Configuration		
Service Accounts		
Service: SQL Server Agent		
Account name	NT Service¥SQLSERVERAGENT	
Startup type	Manual	
Service: SQL Server Database Engine		
Account name	NT Service¥MSSQLSERVER	
Startup type	Automatic	
Service: SQL Server Analysis Services		
Account name	NT Service¥MSSQLServerOLAPService	
Startup type	Automatic	
Service: SQL Server Reporting Services		
Account name	NT Service¥ReportServer	
Startup type	Automatic	
Service: SQL Server Integration Services 12.0		
Account name	NT Service¥MsDtsServer120	
Startup type	Automatic	
Service: SQL Server Distributed Replay Client		
Account name	NT Service¥SQL Server Distributed Replay Client	
Startup type	Manual	
Service: SQL Server Distributed Replay Controller		
Account name	NT Service¥SQL Server Distributed Replay Controller	
Startup type	Manual	
Service: SQL Full-text Filter Daemon Launcher		
Account name	NT Service¥MSSQLFDLauncher	
Startup type	Manual	
Service: SQL Server Browser		
Account name	NT AUTHORITY¥LOCAL SERVICE	
Startup type	Disabled	
Collation		
Database Engine		
collation	Japanese_CI_AS	
Analysis Services		
collation	Japanese_CI_AS	

Database Engine Configuration			
	Server Configuration		
		Authentication Mode	Windows authentication mode
		Specify SQL Server administrators	Administrator
	Data Directories		
		Data root directory	C:¥Program Files¥Microsoft SQL Server¥
		User database directory	C:¥Program Files¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER¥MSSQL¥Data
		User databaselog directory	C:¥Program Files¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER¥MSSQL¥Data
		Temp DB directory	C:¥Program Files¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER¥MSSQL¥Data
		Temp DB log directory	C:¥Program Files¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER¥MSSQL¥Data
		Backup directory	C:¥Program Files¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER¥MSSQL¥Backup
	FILESTREAM		
		Enable FILESTREAM for Transact-SQL access	Disabled
Analysis Services Configuration			
	Server Configuration		
		Server Mode	Multidimensional and data mining mode
		Spacify which users have administrative permissions for Analys	Administrator
	Data Directories		
		Data directory	C:¥Program Files¥Microsoft SQL Server¥MSAS12.MSSQLSERVER¥OLAP¥Data
		Log file directory	C:¥Program Files¥Microsoft SQL Server¥MSAS12.MSSQLSERVER¥OLAP¥Log
		Temp directory	C:¥Program Files¥Microsoft SQL Server¥MSAS12.MSSQLSERVER¥OLAP¥Temp
		Backup directory	C:¥Program Files¥Microsoft SQL Server¥MSAS12.MSSQLSERVER¥OLAP¥Backup
Reporting Services Configuration			
	Reporting Services Native Mode	Install only.	
	Reporting Services SharePoint Integrated Mode	Install only.	
Distributed Replay Controller			
	Spacify which users have permissions for the Distributed Replay C	Administrator	
Distributed Replay Client			
	Controller Name		Blank
	Working Directory	C:¥Program Files (x86)¥Microsoft SQL Server¥DReplayClient¥WorkingDir¥	
	Result Directory	C:¥Program Files (x86)¥Microsoft SQL Server¥DReplayClient¥ResultDir¥	

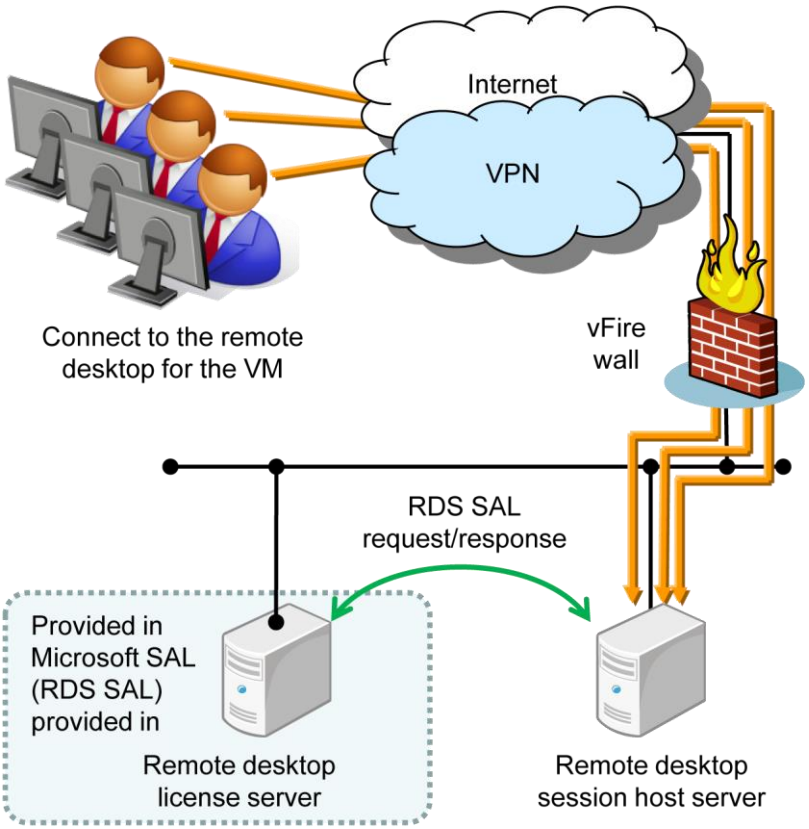
For SQL Server 2014 Standard English

Item	Settings Information	Remark
Feature Selection		
Instance Features		
Database Engine Services	Selected	
SQL Server Replication	Selected	
Full-Text and Semantic Extractions for Search	Selected	
Data Quality Services	Selected	
Analysis Services	Selected	
Reporting Services - Native	Selected	
Shared Features		
Reporting Services - SharePoint	Selected	
Reporting Services Add-in for SharePoint Products	Selected	
Data Quality Client	Selected	
Client Tools Connectivity	Selected	
Integration Services	Selected	
Client Tools Backwards Compatibility	Selected	
Client Tools SDK	Selected	
Documentation Components	Selected	
Management Tools - Basic	Selected	
Management Tools - Complete	Selected	
Distributed Replay Controller	Selected	
Distributed Replay Client	Selected	
SQL Client Connectivity SDK	Selected	
Instance root directory	C:¥Program Files¥Microsoft SQL Server¥	
Shared Feature directory	C:¥Program Files¥Microsoft SQL Server¥	
Shared Feature directory (x86)	C:¥Program Files (x86)¥Microsoft SQL Server¥	
Instance Configuration		
Instance	Default instance	
Instance ID	MSSQLSERVER	
Server Configuration		
Service Accounts		
Service:SQL Server Agent		
Account Name	NT Service¥SQLSERVERAGENT	
Startup Type	Manual	
Service:SQL Server Database Engine		
Account Name	NT Service¥MSSQLSERVER	
Startup Type	Automatic	
Service:SQL Server Analysis Services		
Account Name	NT Service¥MSSQLServerOLAPService	
Startup Type	Automatic	
Service:SQL Server Reporting Services		
Account Name	NT Service¥ReportServer	
Startup Type	Automatic	
Service:SQL Server Integration Services 12.0		
Account Name	NT Service¥MsDtsServer120	
Startup Type	Automatic	
Service:SQL Server Distributed Replay Client		
Account Name	NT Service¥SQL Server Distributed Replay Client	
Startup Type	Manual	
Service:SQL Server Distributed Replay Controller		
Account Name	NT Service¥SQL Server Distributed Replay Controller	
Startup Type	Manual	
Service:SQL Full-text Filter Daemon Launcher		
Account Name	NT Service¥MSSQLFDLauncher	
Startup Type	Manual	
Service:SQL Server Browser		
Account Name	NT AUTHORITY¥LOCAL SERVICE	
Startup Type	Disabled	
Collation		
Database Engine		
collation	SQL_Latin1_General_CP1_CI_AS	
Analysis Services		
collation	Latin1_General_CI_AS	

Database Engine Configuration			
	Server Configuration		
		Authentication Mode	Windows authentication mode
		Spacify SQL Server administrators	Administrator
	Data Directories		
		Data root directory	C:¥Program Files¥Microsoft SQL Server¥
		User database directory	C:¥Program Files¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER¥MSSQL¥Data
		User databaselog directory	C:¥Program Files¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER¥MSSQL¥Data
		Temp DB directory	C:¥Program Files¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER¥MSSQL¥Data
		Temp DB log directory	C:¥Program Files¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER¥MSSQL¥Data
		Backup directory	C:¥Program Files¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER¥MSSQL¥Backup
	FILESTREAM		
		Enable FILESTREAM for Transact-SQL access	Disabled
Analysis Services Configuration			
	Server Configuration		
		Server Mode	Multidimensional and data mining mode
		Spacify which users have administrative permissions for Analysis Services	Administrator
	Data Directories		
		Data directory	C:¥Program Files¥Microsoft SQL Server¥MSAS12.MSSQLSERVER¥OLAP¥Data
		Log file directory	C:¥Program Files¥Microsoft SQL Server¥MSAS12.MSSQLSERVER¥OLAP¥Log
		Temp directory	C:¥Program Files¥Microsoft SQL Server¥MSAS12.MSSQLSERVER¥OLAP¥Temp
		Backup directory	C:¥Program Files¥Microsoft SQL Server¥MSAS12.MSSQLSERVER¥OLAP¥Backup
Reporting Services Configuration			
	Reporting Services Native Mode	Install only.	
	Reporting Services SharePoint Integrated Mode	Install only.	
Distributed Replay Controller			
	Spacify which users have permissions for the Distributed Replay Controller service	Administrator	
Distributed Replay Client			
	Controller Name		Blank
	Working Directory	C:¥Program Files (x86)¥Microsoft SQL Server¥DReplayClient¥WorkingDir¥	
	Result Directory	C:¥Program Files (x86)¥Microsoft SQL Server¥DReplayClient¥ResultDir¥	

3.6 Microsoft SAL (RDS SAL)

Microsoft SAL (RDS SAL) is a service that provides a Microsoft Remote Desktop Service Subscriber Access License (called an "RDS SAL" below) on Virtual Machines created in Compute Resource. This makes it possible for three or more users to connect to a remote desktop (Remote desktop session host server. Windows Server) for a specific Virtual Machine in Compute Resource.


Internet
VPN
Connect to the remote desktop for the VM
vFire wall
RDS SAL request/response
Provided in Microsoft SAL (RDS SAL) provided in
Remote desktop license server
Remote desktop session host server

INFO

- In Microsoft SAL (RDS SAL), NTT Communications provides RDS SALs as its own service, based on a contract signed under Microsoft's SPLA license agreement.

3.6.1 Available Features

You can use the following features in Microsoft SAL (RDS SAL).

Provided Feature	Feature Overview
Provision of an RDS SAL	A feature that uses an RDS SAL to allow a remote desktop connection for three or more users for a specific Virtual Machine (Windows Server) in Compute Resource.
Provision of a Public Catalog	A feature that uses a template of the Virtual Machine to provide the above license.

3.6.2 Provision of an RDS SAL

The RDS SALs provided by Microsoft SAL (RDS SAL) are shown below.

Item	Details
Version	Windows Server 2008 R2 Remote Desktop Services SAL
Quantity	10, 30, 50, or 100
Type	User SAL

3.6.3 Provision of a Public Catalog

You can use the templates provided by the RDS SAL to create a Virtual Machine (remote desktop license server).

You can use templates from the Customer Portal when creating a Virtual Machine in Compute Resource or Compute Resource (Dedicated Device).

NOTE

- An RDS SAL is only provided for a Virtual Machine created using the provided template (called a "Virtual Machine created with Microsoft SAL (RDS SAL)" below).
- One RDS SAL and one OS license are provided as a set for one Virtual Machine created using Microsoft SAL (RDS SAL).

  The OS that is provided in the set is "Windows Server 2008 R2 Enterprise Japanese/English (64 bit version)." For details regarding the conditions for providing an OS license, refer to "3.4 OS License" (⇒ P.92).

INFO

- Templates exist for each Data Center and are stored in the Public Catalog, which can be accessed by all users of that Data Center.

3.6.4 Important Points

- The required number of licenses is the "number of total users that might connect," not the "number that will connect at the same time." Failure to purchase enough licenses is a license violation.
- We recommend use in a domain environment with the specifications formulated by Microsoft.
- To increase or decrease RDS SALs, add or delete servers. Please add or delete the servers yourself. NTT Communications cannot perform these features.
- The system requirements (number of vCPUs, Memory capacity, and Disk capacity) for the Virtual Machine (remote desktop license server) are listed below.

Item	Quantity
vCPU	1 or more
Memory capacity	2 GB or greater
Disk capacity	100 GB or greater

- For information on settings for the remote desktop session host server, refer to the user's manual provided by NTT Communications.
- Setting up a remote desktop session host server in an On-Premises Environment to ask a Virtual Machine (remote desktop license server) created using Microsoft SAL (RDS SAL) for a RDS SAL is prohibited based on the license restrictions.

Prohibited Acts

The acts listed below violate the agreement between the user and Microsoft, or are considered incorrect usage of NTT Communications services. Users engaged in such acts may be subject to penalties imposed by NTT Communications such as suspension of service, or incorrect usage penalties imposed by Microsoft.

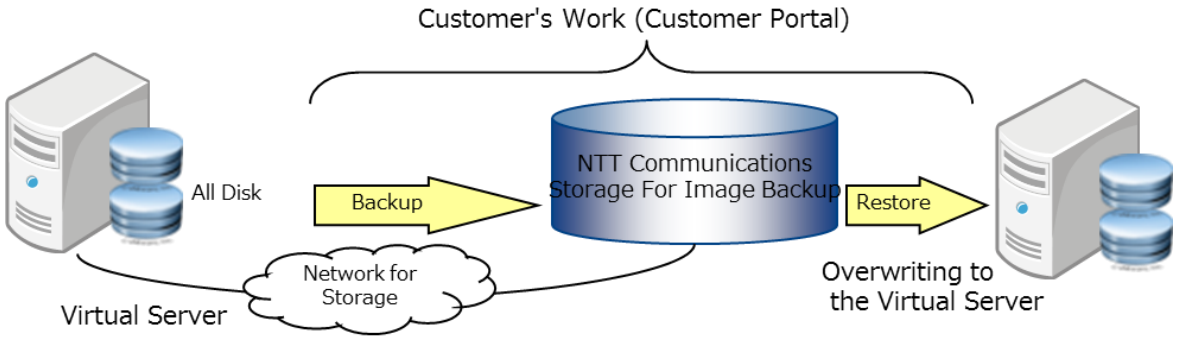
The following acts are specific examples. The acts that may be subject to penalties are not limited to the acts below.

- Using licensed products provided through Microsoft SAL (RDS SAL) outside of the cloud environment specified by NTT Communications.
- Using the Customer Portal features to create and save another template of the Virtual Machine image, using the export feature to store the template outside of the NTT Communications cloud environment, creating a new Virtual Machine based on that file, and running licensed products that have been provided by NTT Communications.
- Duplicating and using the software without notifying NTT Communications.
- Using Microsoft SAL (RDS SAL) to duplicate the image of the Virtual Machine that you are running and then running it as another Virtual Machine without notifying NTT Communications.

4. Backup (Global Standard Menu)

4.1 Image Backup

Image Backup is a service that provides features to acquire and store Virtual Server images (called "Backup Images" below) and features to restore the Virtual Server from the stored backup images.



NOTE

- You can use image backup at a Data Center that provides Compute Resource or Compute Resource (Dedicated Device).The products provided differ depending on the Data Center. For details, refer to "1.3.2 Available Data Centers" (⇒P.21).

4.1.1 Available Features

Customer can use the following features in Image Backup.

Function	Outline
Backup and Restore	A feature that acquires, stores and restores backup images for the purpose of backup. Backup images are stored in a storage device provided by the NTT Communications (called "Backup Storage" below). For restoration, backup images are directly overwritten on the Virtual Server.
Backup and Restore Management	A feature that manages backup of the Virtual Server. It is possible to manage the schedule and check the history of backup and restore.

4.1.2 Backup and Restore

Backup

A feature that acquires and stores backup images for the purpose of backup of the Virtual Server. Disk images for backup are acquired and stored in backup storage after the backup starts. Following are disks for backup.

- All disks for the Virtual Server

- Image Backup does not support Virtual Machine which is over 4,000GB for total disk capacity + the memory resource (different for each Compute Class).

Restore

Backup image is overwritten on and restored from the Virtual Server from which backup is acquired.

INFO

- The Virtual Server is restored at the state of Power Off. The Virtual Server needs to be manually started.

The restored Virtual Server is restored with the following settings for vCPU, memory, disk and vNIC.

Item	Description of setting
vCPU	Restores the configuration of the Virtual Server targeted for backup.
Memory	Restores the configuration of the Virtual Server targeted for backup.
Disk	Restores the configuration of the Virtual Server targeted for backup.
vNIC	Restores the vNIC information of the Virtual Server targeted for backup (IP address, net mask, Mac address).

NOTE

- For various settings of Guest OS, settings of the Virtual Server targeted for backup are restored, but some setting items including default GW, subnet mask and DNS are not backed up. For details, refer to "Guest OS Customization" (⇒P.66).
- The "change S-ID" (Sysprep) that is normally performed while using Windows is not performed.

4.1.3 Backup and Restore Management

A feature for referencing the schedule and job history relevant to backup and restore and a feature for managing backup image are provided. Job indicates processing related to backup and restore. When the image backup job is completed, the result is automatically reported via E-mail.

Schedule Management Function

This is a feature that manages backup job. It is possible to create the backup job by specifying the schedule type, retention period and start date, or change or delete the created backup job.

Name	Description
Effective flag (Schedule)	It is possible to enable or disable this backup job.
Job history (Scheduled jobs)	It is possible to select the job from the schedule configured in the past or configure a new schedule. If the job is selected from the schedule configured in the past, the configured contents are adopted.
Schedule type	It is possible to select the spot (One-Time), daily, weekly and monthly backup time.
Retention period	You can decide the retention period for the acquired backup image. Retention period varies depending on schedule type.
Date	You can specify the date from when backup starts. For spot, daily and monthly backup, the start date can be configured. For the weekly backup, the starting day of week can be configured. For the monthly backup, the third Monday can be configured.
Time slot	24 hours can be specified in units of 1 hour.
Backup time	Either image backup or file backup can be selected.

NOTE

- While the effective flag is disabled, backup does not start.
- Time slot is the estimate of the time when backup starts so that time is not guaranteed.

The backup job can be created in units of Virtual Server and it is possible to create one backup job after combining multiple Virtual Servers.

Backup Schedule

With the schedule management function, retention time, date and time slot can be specified for each schedule type. For backup, only the method that starts the backup at the specified time slot is available. Time can be specified at the local time when backup is acquired.

- Setting the retention period, date and time slot for each schedule type

Schedule type	Retention time	Date *4	Time slot *2
Spot	1 day, 31 days, 366 days	Specifying the date (Calendar date)	0 to 1, 1 to 2, 2 to 3, 3 to 4, 4 to 5, 5 to 6, 6 to 7, 7 to 8, 8 to 9, 9 to 10, 10 to 11, 11 to 12 12 to 13, 13 to 14, 14 to 15, 15 to 16, 16 to 17, 17 to 18, 18 to 19 19 to 20, 20 to 21, 21 to 22, 22 to 23, 23 to 24
Daily	1, 2, 3, 4, 5, 6, 7 and 8 days	Specifying the date (Calendar date)	
Weekly	7, 14, 21, 28, 35, 42, 49 and 56 days	Specifying the date (Specifying the day of week on which backup is acquired)	
Monthly	31, 62, 93, 124, 155, 186, 217 and 248 days	The specific day is specified.*1 (Example: Second Wednesday) Or the date is specified (1st to 31st, the last day)	

*1 If the combination between ordinal numbers and day of week is not correct, backup does not start.

* Specification of date and time slot is dependent on the preconfigured time zone.

Virtual Server Management Function

For the registered Virtual Server, it is possible to check the configuration to confirm whether the backup job is enabled.

Displaying the History of Backup and Restore

History of execution of backup and restoration is displayed. History is displayed in order of time when job starts, job type (backup or restore), status (Success/Failed), execution time and target Virtual Server. Following 2 display methods: history display for the latest 7 days and all history display.

Backup Image Management and Restore

List of backup image is displayed. The list displays start time, end time, image size and disk type (all disks). Restore can be executed from the list. Restore is

immediately executed. It is also possible to delete the backup image immediately.

4.1.4 Important Points

Backup Image Store

- Image backup supports following Guest OS license Virtua Server templetes provided by NTT Communications.

Windows Server 2008 R2 Enterprise Windows Server 2012 Standard
Red Hat Enterprise Linux Server 5.8/6.2

- The backup image storage capacity is the size of the Disk of the Virtual Server targeted for backup. It is different from the data capacity written into the backup storage.

NOTE

- When Virtual Server is deployed from Virtual Server template backup jobs cannot be set immadiately. From a first power on, please wait for about 2 hours and set.
- The Virtual Server is charged according to disk size.
- The starting point of the retention period for backup storage is the start time of the backup. Charging starts from that point. No fee is charged if backup fails.

- The Backup Image acquisition process is performed independently of whether the Virtual Server targeted for backup is powered on or off.
- During backups, the performance of the Disk I/O of the Virtual Server that is being backed up might be reduced.
- The backup begins within the Time Window you specify. The backup start time cannot be specified in units of minutes and seconds.
- Backup cannot be configured in the last 5 minutes (55 minutes to 0 minute) of the 1-hour time slot for backup. (The alert message appears.)
- If the number of backup jobs that are performed at the same time in each time slot exceeds the maximum value, we recommend using the closest available time slot within the same day or the closest date in the same time slot.
- If the Virtual Server targeted for backup has been deleted at the backup start time, the backup will not be performed.
- Disk of the target Virtual Server cannot be extended while performing the backup process.

- To ensure consistency of the file system during backup, we recommend setting rest points, such as turning OFF the Virtual Server, and performing the backup.

NOTE

- When Virtual Server is shut down by Cutomer Portal or in Guest OS, status is change to Partially Powered Off. So please push Power Off button by Customer Portal mandatory in order to complete to be powered off.

- If the target Virtual Server is restored during the backup, inconsistency in backup data may occur so do not perform the restore operation during the backup.
- When restoring the backup, old root/Admin passwords used when performing the backup are enabled. Be careful not to forget old passwords because you cannot log in to the Virtual Server if you do not know these old passwords.
- Backup image is stored in the storage for backup during the retention period specified by customer and the image is deleted when the retention period expires. The retention period cannot be extended.
- Backup image cannot be acquired while External Storage is being mounted. Please make sure to backup after the unmount. When restoring, please remount again.

Backup Image Restore

- For restore, backup image is overwritten on and restored from the Virtual Server from which backup is acquired.

NOTE

- It may take some time for Guest OS Customization at the initial start-up after the restore. Please start the operation after 15 minutes, once you have confirmed the status as “Successful” on the Backup Report for the Customer Portal or received the Restore Completion Mail (If the mail receive setting is valid) Restore operation cannot be performed if the target Virtual Server is deleted.
- Please do not operate the Virtual Machine(such as changing SID etc.) before the initial power on when restoring.Performance and Statistic Report from the past will be deleted.

- After a restore NIC parameter in Guest OS may be chanded. It cannot affect the communication, but, please contact support desk when there is some inconvenience.
- When disk of Virtual Server under operation is deleted after backup and the disk contract of Compute Resource is being reduced, please perfrom restoration after cheking wheter the amount of disks required for restoration is secured in Compute Resource.
- Please exexute the VM restoration one by one within same Compute Resource Pool. It is necessary to have free memory on Compute Resource Pool for overhead only when restoring. (The overhead is recommended to be max. 20% of the memory assigned to the Virtual Machine.)

- If the IP Address for Virtual Machine is assigned either on vFirewall or vLoadBalancer, please release the settings of vFirewall or vLoadbalancer temporarily and restore. Please contact the Support Center via Customer Portal ticket, if the restoration does not complete.
- Please do not assign the IP Address of the Virtual Machine used during the Backup to other Virtual Machines. Restoration will fail due to IP Address duplication.

Backup of Compute Resource (Dedicated Device)

Be careful with the following points when backing up the Virtual Server used by Compute Resource (Dedicated Device).

- For the backup work area, 10% of the Storage Device that is used by Compute Resource (Dedicated Device) will be used.
- During the backup, the performance of the Disk I/O of the Storage Device that is used by Compute Resource (Dedicated Device) may decrease temporarily.
- Backup of Compute Resource (Dedicated Device) may not be supported depending on usage of disk I/O so please contact us.

License of the Restored Virtual Server

- If the Virtual Server targeted for backup was using the OS license provided by NTT Communications, the overwritten restored license on the Virtual Server is equivalent to the OS license. Therefore, no OS license is added to the restored Virtual Server.

Guest OS Setting

When changing the Guest OS network settings, do not disable a vNIC that has been recognized, even if you are not using that vNIC. If Virtual Servers with disabled vNIC are backed up and restored, failures might occur.

Difference between the Setting Time and Chargeable Duration due to Difference of Time Zone

Configurable date and time slot are set on the Portal window according to the local time (configured time zone). However, the system operated with the universal time coordinated (UTC) so that charging is processed with UTC. For Japan, backup process that takes a maximum of 9 hours is charged as the process for the previous day.

Example) Charging when backup is performed at the end of month in the Japanese time zone

To make the explanation easy to understand, Japan Standard Time (JST) is set for time zone, backup date is set to 0:00 on April 1 (Japan Standard Time) and 0 minute is set for the backup period.

If the backup retention period is set to one day, the data retention period is set from 0:00 to 23:59 on April 1 in Japan Standard Time. However, if the period is converted with UTC, the period is converted to (1) 15:00 to 23:59 on March 31 and (2) 00:00 to

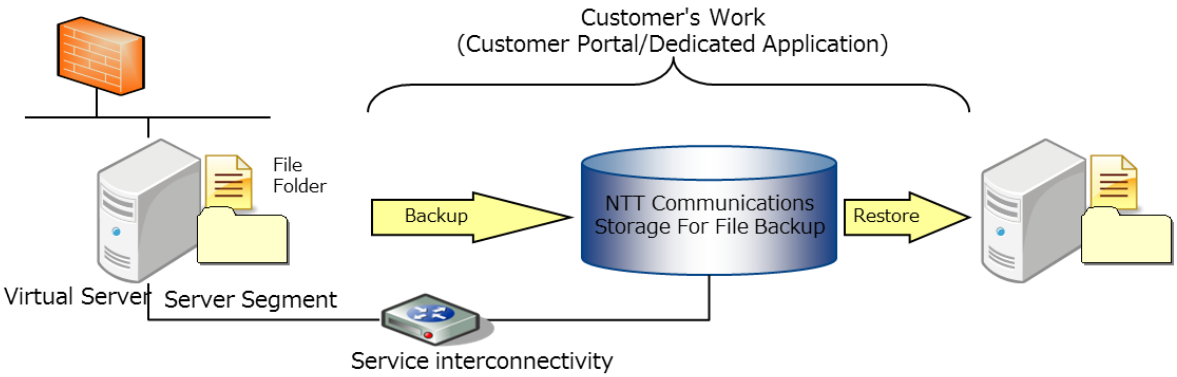
14:59 on April 1. Therefore, (1) is processed as the fee for March and (2) is processed as the fee for April. The time notation in the E-mail about the result of job is UTC.

When Using OS Management

If the OS management service is used, you cannot use the image backup service.

4.2 File Backup

File Backup is a service that provides features to store and restore files or folders on the data disk of the Virtual Server (called "Backup file" below").



NOTE

- You can use file backup at a Data Center that provides Compute Resource or Compute Resource (Dedicated Device).The services provided differ depending on the Data Center. For details, refer to "1.3.2 Available Data Centers" (⇒P.21).
- File backup uses the Service Interconnectivity and the Server Segment.
- Order Form is needed for this service derivery.

4.2.1 Available Features

You can use the following features in File Backup.

Function	Outline	Operation
Backup File Storage	A feature for acquiring backup files from and storing backup files in the storage device (called "storage for backup") provided by NTT Communications.	Customer Portal
Backup File Restore	A feature for restoring the backup file* This feature is available from the dedicated application, NetBackup Agent (called "NBU Agent" below), which is installed in the Virtual Server.	Dedicated Application (Use Remote Console or RDP and SSH.)
Backup and Restore Management	A feature that manages backup. A feature for realizing management of files and folders targeted for backup, schedule management and history management.	Customer Portal

4.2.2 Backup File Storage

Backup files are stored in backup storage at the time of start time. Backup file is stored in the storage for backup during the retention period specified by customer and the file is automatically deleted when the retention period expires.

Specifying Backup File

When specifying the backup file, Virtual Server needs to be selected and the path of the file or folder targeted for backup needs to be entered when configuring the backup job in the Customer Portal.

Encrypting Backup File

The backup file is automatically encrypted by using NBU Agent and the file is stored in the storage for backup. The encryption key needs to be generated by using NBU Agent. Encryption cannot be disabled.

If the encryption key is lost, the same encryption needs to be generated again when restoring the backup file. In this case, the encryption key needs to be generated by using the same pass phrase as that of the original encryption key.

NOTE

- Keep the pass phrase with care because the backup file cannot be restored if you forget the pass phrase.

- Setting the retention period, date and time slot for each schedule type

Schedule type	Full backup/ incremental backup	Retention period	Date *4	Time slot *2
Spot	Full backup	1 day, 31 days, 366 days	Specifying the date (Calender date)	0 to 3,3 to 6,6 to 9,9 to 12,12 to 15,15 to 18,18 to 21,12 to 24
Daily	Full backup	1, 2, 3, 4, 5, 6, 7 and 8 days	Specifying the day of week (Calender date)	
Weekly	(1) Weekly full backup	7, 14, 21, 28, 35, 42 and 56 days	Specifying the date (Specifying the day of week on which backup is acquired)	
	(2) Weekly full backup + daily incremental backup	7, 14, 21, 28, 35, 42 and 56 days		
Monthly	Full backup	31, 62, 93, 124, 155, 186, 217 and 248 days	The specific day is specified*1. (Example: Second Wednesday) Or the date is	

	specified (1st to 31st, the last day)

*1 If the combination between ordinal numbers and day of week is not correct, backup does not start.

* Specification of date and time slot is dependent on the preconfigured time zone.

4.2.3 Backup File Restore

Backup file can be restored on the Virtual Server from which backup is acquired.

NOTE

- This function cannot be operated from the Customer Portal. This process can be executed from the NBU Agent installed on the Virtual Server. Refer to the User Guideline for details of how to operate the NBU Agent.
- Restore can be done on the Virtual Server from which backup is acquired. Be careful that no file can be restored if the target Virtual Server is deleted.
- Restore can be done on the same file (or folder) by overwriting or newly another space on the same Virtual Server. Overwriting is recommended in this service. If overwriting is selected, same amount of blank disk is needed to restore.

4.2.4 Backup and Restore Management

A feature for managing the schedule and job history relevant to file backup and restore and a feature for managing backup file are provided. After backup job is finished, result E-mail will be delivered.

Schedule Management Function

A feature that manages the backup job. It is possible to create the backup job by specifying the schedule type, retention period and start date, or change or delete the created backup job.

Name	Description
Effective flag (Schedule)	It is possible to enable or disable this backup job.
Job history	It is possible to select the job from the schedule configured in the past or configure a new schedule. If the job is selected from

(Scheduled jobs)	the schedule configured in the past, the configured contents are adopted.
Schedule type	It is possible to select the spot (One-Time), daily, weekly and monthly backup time.
Incremental backup*	If the weekly backup is selected for the schedule type, combination with daily incremental backup can be selected.
Retention period	You can decide the retention period for the acquired backup image. Retention period varies depending on schedule type.
Date	You can specify the date from when backup starts. For spot, daily and monthly backup, the start date can be configured. For the weekly backup, the starting day of week can be configured. For the monthly backup, the third Monday can be configured.
Time slot	24 hours can be specified in units of 3 hours.
Backup target path	Enter the path of the file or folder targeted for backup. Multiple paths can be described simultaneously by starting new lines. (Example: /usr/local (for Linux) and c:¥Program Files (for Windows), etc.) * Although the backup schedule is registered even if the path that does not exist in the Virtual Server is entered, please note that backup will not be executed. And if file or folder name is changed after backup job was set, backup job will not be excuted.
Backup type	Either image backup or file backup can be selected.

※ Full backup is executed once a week and daily incremental backup is executed for backing up images or files added from the previous day. With combination of weekly full backup and daily incremental backup, usage fee can be saved compared to the fee charged when full backup is executed every day.

NOTE

- While the effective flag is disabled, backup does not start.
- Time slot is the estimate of the time when backup starts so that time is not guaranteed.

INFO

- The backup job can be created as one backup job by combining multiple files and folders existing in a single VM or multiple VMs.

Virtual Server Management Function

For the Virtual Server registered as the target of file backup, it is possible to check the configurations to confirm whether the backup job is enabled. It is possible to move from this feature to the schedule management feature and then set a new schedule.

Backup History

History of execution of backup is displayed. History is displayed in order of time when job starts, job type (backup), status (Success/Failed), execution time and target file/folder. Following 2 display methods: history display for the latest 7 days and all history display. Restore can be executed only from the NBU Agent installed on the Virtual Server. Restore history can be displayed by NBU Agent.

Restore Management

The backup file list (start time, end time disk type (all disks)) can be checked and restored from the NBU Agent. Restore is immediately executed. It is also possible to delete the backup file immediately.

4.2.5 Important Points

About Application for this Service

- To use this service, you must provide information about ID/password with administrator right or root right for the Virtual Server containing file and folder targeted for file backup to NTT Communications. NTT Communications use this information for installing and configuring NBU Agent. Be sure to delete ID or change password immediately after NBU Agent becomes available.
- In addition to installation and configuration of NBU Agent, the work for registering information of the targeted Virtual Server into the NTT Communications' backup infrastructure is necessary. Even if the customer configures NBU Agent, this service is not available until NTT Communications completes the above registration work.
- NTT Communications set up Server Segment for File Backup. If Customer have already used IP address range below, this service cannot be provided.
  - 10.223.112.0/20
- Please permit port 1556 for this servce. Please refer to following site in case of Windows Firewall settings.

  http://windows.microsoft.com/ja-jp/windows/understanding-firewall-settings#1TC=windows-7
- Please do not change any Server Segment parameter for Filebackup by Customer Portal.
- In Windows Server Registry Key will be added for this service. Please confirm whether there isn't influence to the system beforehand.

Registory Key	Parameter

REQESTED_INTERFACE	Host Name (for backup Server Segment)
CRYPT_OPTION	REQIRED (Fixed)
CRYPT_KIND	STANDARD (Fixed)
CRYPT_CIPHER	AES-256-CFB (Fixed)

NOTE

- On the derivery process reboot and Guest OS Customization are needed. Some parameters will be changed. For details, refer to "Guest OS Customization" (⇒P.66).
- Server Segment for this service is reserved. Please do not use for other uses.

Recommended Environment

- File backup supports following Guest OS license Virtual Server Templates provided by NTT Communications.

Windows Server 2008 R2 Enterprise Windows Server 2012 Standard
Red Hat Enterprise Linux Server 5.8/6.2

- NTT Communications does not support the Guest OS described below.

  http://www.symantec.com/ja/jp/netbackup/system-requirements

- The Virtual Server in which NBU Agent is installed requires approximately 1.5GB of free disk capacity and a memory with a minimum of 512MB.

Backup File Storage

- The backup image storage capacity is the size of the file targeted for backup. It is different from the data capacity written into the backup storage.
- The backup job can be created as one backup job by combining multiple files and folders existing in a single Virtual Server or multiple Virtual Servers. The total size of the Virtual Server targeted for one backup job (this is not the size of the file/folder) is up to 1500GB. If multiple Virtual Servers exceeding 1500GB are selected, 2 or more backup jobs need to be provided.
- The Backup File acquisition process is performed only if the Virtual Server targeted for backup is powered on.

- During backups, the performance of the Disk I/O of the Virtual Server that is being backed up might be reduced.
- The backup begins within the time slot you specify. The backup start time cannot be specified in units of minutes and seconds.
- Backup cannot be configured in the last 5 minutes (55 minutes to 0 minute) of the 3-hour time slot for backup. (The alert message appears.)
- If the number of backup jobs that are performed at the same time in each time slot exceeds the maximum value, we recommend the closest available time slot within the same day or the closest date in the same time slot.
- If the Virtual Server targeted for backup has been deleted at the backup start time, the backup will not be performed.
- Disk of the target Virtual Server cannot be extended while performing the backup process.
- The starting point of the retention period for backup file is the start time of the backup.
- If the target Virtual Server is restored during the backup, inconsistency in backup data may occur so do not perform the restore operation during the backup.
- When backup is acquired periodically, there might be a time period without the backup file due to the gap between the start time of next backup and retention period. In order to avoid this situation, one additional day will be added to the retention period with no charge.

Backup of Compute Resource (Dedicated Device)

Be careful with the following points when performing the file backup for the Virtual Server used by Compute Resource (Dedicated Device).

- During the backup, the performance of the Disk I/O of the Storage Device that is used by Compute Resource (Dedicated Device) may decrease temporarily.
- Backup of Compute Resource (Dedicated Device) may not be supported depending on usage of disk I/O. In this case, please contact our Support Center.

Difference between the Setting Time and Chargeable Duration due to Difference of Time Zone

Configurable date and time slot are set on the Portal window according to the local time (configured time zone). However, fee is charged based on the universal time coordinated (UTC) in consideration of specifications of the service. For Japan, backup process that takes a maximum of 9 hours is charged as the process for the previous day due to a time difference.

Example) Charging when backup is performed at the end of month in the Japanese time zone

Japan Standard Time (JST) is set for time zone; backup date is set to 0:00 on April 1 (Japan Standard Time) and 0 minute is set for the backup period.

If the backup retention period is set to one day, the data retention period is set from 0:00 to 23:59 on April 1 in Japan Standard Time. However, if the period is converted with UTC, the period is converted to (1) 15:00 to 23:59 on March 31 and (2) 00:00 to 14:59 on April 1. Therefore, (1) is processed as the fee for March and (2) is processed as the fee for April.

A half-width kana character cannot be specified in backup and restore. (Japan only)

The file and folder using a half-width kana character cannot be backed up.

5. Network Features (Global Standard Menu)

5.1 Internet Connectivity

Internet Connectivity is a service that provides customers using Enterprise Cloud with Internet Connectivity constructed with redundant equipment. Also, we provide Global IP Addresses that are required for Internet communication.

NOTE
- The products provided differ depending on the Data Center. For details, refer to "1.3.2 Available Data Centers" (⇒P.21).

5.1.1 Available Features

The following features are available for Internet Connectivity.

Feature	Overview
An Internet GW is provided	vFirewall provided by vFirewall and gateway feature that connects to the Internet (called "Internet GW" below).
Global IP Addresses are Provided	A feature that uses Global IP Addresses that are required for Internet communication.

5.1.2 An Internet GW Is Provided

The Internet GW is a gateway that connects the vFirewall provided by vFirewall with the Internet.

You can choose from the following connection plans to match your required transmission speed.

Connection Plan	Overview
10 Mbps Best Effort	Transmission speed: Provides maximum speed of 10 Mbps.
100 Mbps Best Effort	Transmission speed: Provides maximum speed of 100 Mbps.
1 Gbps Best Effort	Transmission speed: Provides maximum speed of 1 Gbps.

Guaranteed	Provides guaranteed transmission speed with the specified bandwidth as the upper limit. You can specify any of the following bandwidths. ● 1 to 10 Mbps (You can specify it in 1 Mbps increments.) ● 15 Mbps ● 20 Mbps ● 25 Mbps ● 30 Mbps ● 40 Mbps ● 50 Mbps ● 60 Mbps ● 70 Mbps ● 80 Mbps ● 90 Mbps ● 100 Mbps ● 200 Mbps ● 300 Mbps ● 500 Mbps ● 700 Mbps ● 1 Gbps

NOTE

- The Best Effort Type is a best effort type service that changes the transmission speed according to your system environment and line congestion. The actual transmission speed varies according to the usage of other customers and infrastructure status. The service does not guarantee transmission speed.
- The Guaranteed type does not provide transmission speed higher than the specified bandwidth.

INFO

- The Internet GW is constructed of redundant physical devices (equipment and lines).
- It supports Internet protocol version IPv4.

5.1.3 Global IP Addresses Are Provided

You can use Global IP Addresses that are required for Internet communication.

You can specify the following numbers of Global IP Addresses. Global IP Address is provided to customer differently whether they select vFirewall or Integrated Network Appliances.

重要

- Customer cannot assign the provided Global IP Address. Also, customer cannot change the provided Global IP Address.

メモ

- Global IP Address will be assigned according to NTTCom's Global IP Address Block.

For Customer using vFirewall,

If the customer is using vFirewall, Global IP would be provided as follows. The distributed Global IP Address can be set as the IP Address for NAT/NAPT rule in the vFirewall.

	Lower Limit	Upper Limit	Setting Unit
Global IP Address	4	64	4

NOTE

- If you order 8 or more Global IP Addresses, the IP Addresses might not be sequential.
- If you use 65 or more IP Addresses, please consult with us separately.

For Customer using Integrated Network Appliance,

If the Customer is using the Integrated Network appliance, Global IP can be purchased according to the following subnet units. The Global IPs will be assigned to the Internet Transit and will be used for transmission between each devices connected to the Internet Transit. Also, Global IPs can be utilized for the NAT, Load Balancing and IPsec termination rules.

	Subnet	Available number of rules set for NAT/NAPT, Load Balancing, and IPsec termination
Global IP Address	/29	3
	/28	11
	/27	27

重要

- A single subnet contract can be made for a single Internet Connectivity contract.
- Customer can assign either one of the subnet when making a contract for Internet Connectivity service. The Global IP subnet cannot be changed after the Internet Connectivity installation.

5.1.4 Important Points

Restrictions When Connecting to the Internet

- Internet Connectivity is a service in which multiple customers share the Internet lines that are made available by NTT Communications. Internet lines that are provided by the customer cannot be used.
- Bandwidths specified with the Guaranteed type are guaranteed for all the Global IP Addresses provided. You cannot specify IP Addresses and guarantee the bandwidth.
- The Guaranteed type only guarantees the communication bandwidths that pass through the Internet GW. In order to guarantee the communication bandwidth that the vFirewall and vLoad Balancer pass through, it is necessary to have separate contracts for a suitable number of firewall resources and load balancer resources.
- Communication interruptions might occur when Internet Connectivity settings are changed.
- This service does not provide DNS resolver. Please prepare DNS by Customer.
- The DNS resolver is not offered with this service. Customer needs to prepare.

Restrictions on Placing Orders

- If you are using DDoS Solution Service (J030801) at Yokohama No.1 Data Center, you cannot use a plan higher than 1 Gbps Best Effort type or 200 Mbps Guaranteed Band type.

  ※ DDos Solution Service is a service that is unique to Japan Data Centers (Local Option Menu).

5.2 VPN Connectivity

VPN Connectivity provides a connection to Arcstar Universal One Service (NTT Communications VPN service). The function of plan change and routing setting and Ping is available on the Customer Portal the service released Data Center.

5.2.1 Available Features

The following features are available for VPN Connectivity.

Feature	Overview
VPN Gateway	A gateway feature (called "VPN Gateway" below) that connects Arcstar Universal One Service to vFirewall or I ntegrated Nework Appliance.
VPN Routing Settings	A feature that sets up routing to enable communication between Arcstar Universal One Service and vFirewall or Integrated Nework Appliance.
Ping	Ping function in VPN Gateway

※ Arcstar IP-VPN Service can be available via Universal One using “Arcster Universal One Connectivity Service”.

5.2.2 VPN Gateway

The VPN Connectivity GW is a gateway that connects Arcstar Universal One Service to vFirewall or Integrated Nework Appliance.

You can choose from the following connection plans to match your required transmission speed.

Connection Plan	Overview
100 Mbps Best Effort	Transmission speed: Provides maximum uplink speed of 100 Mbps and maximum downlink speed of 100 Mbps.
Guaranteed	Provides guaranteed transmission speed with the specified bandwidth (uplink/downlink) as the upper limit. You can specify any of the following bandwidths. ● 100 Mbps ● 200 Mbps ● 1 Gbps

NOTE

- The Best Effort Type is a best effort type service that changes the transmission speed according to your system environment and line congestion. The actual transmission speed varies according to the usage of other customers and infrastructure status. The service does not guarantee transmission speed.
- The Guaranteed type does not provide transmission speed higher than

the specified bandwidth.

INFO
- The VPN Gateway is constructed of redundant physical devices (equipment and lines).
- It supports Internet protocol version IPv4.

5.2.3 VPN Routing Settings

You can set up routing for communication between Enterprise Cloud IP Addresses and Customer location or another Enterprise Cloud Data Center or other application services via VPN.

INFO
- Routing can be set up for a maximum of 128 routes (other than the default routes). But 24 routes are a maximum in Customer Portal available VPN Connectivity.

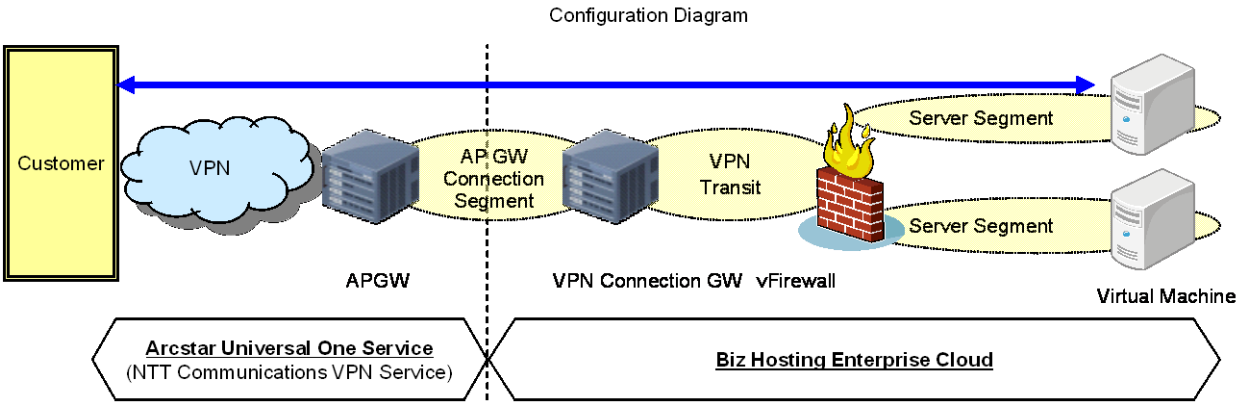
5.2.4 Enterprise Cloud and VPN Routing Design

When you order the service, you must specify the following VPN Connectivity settings.

Item	Overview	Prefix Length of IP Address Blocks
APGW connection segment settings(※1)	Sets the Server Segments (called "APGW connection segments" below) used for connecting between the VPN Gateway and the application gateway (called "APGW" below).	/27
VPN Transit settings	Sets the Server Segments (called "VPN Transit" below) used for connecting between the VPN Gateway and vFirewall or Integrated Nework Appliance.	/29 to /24
Routing settings	Sets up routing to enable communication between Arcstar Universal One Service and vFirewall or Integrated Nework Appliance.	/29 to /8 (※2)

※1 It is not necessary in Customer Portal available VPN Connectivity.

※2 For each route, any one of them is specified.



APGW Connection Segment

- Your VPN IP Address block (called "APGW connection segment IP address block" below) can be allocated to APGW connection segments.
- NTT Communications selects and sets the IP addresses that are allocated to VPN Gateway and APGW from the APGW connection segment IP address block.

VPN Transit

- Your VPN IP Address block (called "IP address block for VPN transit" below) will be allocated to VPN transit.
- NTT Communications selects and sets the IP addresses that are allocated to VPN Gateway and vFirewall or Integrated Nework Appliance from the VPN Transit IP address block.

Routing Settings

- In order to communicate from your VPN to vFirewall or Integrated Nework Appliance, routing is set with vFirewall or Integrated Nework Appliance as the destination.
- IP address block not used in Customers VPN is allocated to the destination network address that is set in the routing settings.
- The network used by Enterprise Cloud service cannot be specified as a default route of VPN service (Arcstar Universal One) side.

NOTE

- You cannot change the IP addresses that are used for VPN transit and APGW conneciton segment after you have started using VPN Connectivity.

5.2.5 Important Points

- The Guaranteed type only guarantees the communication bands that pass through the VPN Gateway. In order to guarantee the communication bandwidth that the vFirewall and vLoad Balancer pass through, it is necessary to have separate contracts for a suitable number of firewall resources and load balancer resources.
- NTT Communications may change VPN settings for maintenance and monitoring. You cannot change or delete the settings that are set by NTT Communications.

- Communication interruptions might occur when VPN Connectivity settings are changed.
- The IP Addresses in the IP Address bands listed below cannot be included in the IP address block for APGW connection segment, IP address block for VPN Transit, or routing IP address block for vFirewall. Be aware that the IP address bands that cannot be specified differ according to Data Center.

  Also, if the IP Addresses in the IP Address bands listed below are used for private network lines, communications between the Data Center that is in use and those IP addresses via vFirewall will not be possible.

Data Center	Non-duplicatable IP Address Bands
Yokohama No.1	172.22.0.0/17 172.22.128.0/17 10.223.0.0/17 10.223.128.0/17
Kansai 1	172.23.0.0/17 10.233.0.0/17 172.23.128.0/17 10.233.128.0/17
Hong Kong Tai Po	172.22.128.0/17 172.31.128.0/17 10.223.128.0/17 10.224.128.0/17
Singapore Serangoon	172.20.0.0/17 10.200.0.0/17 172.20.128.0/17 10.200.128.0/17
San Jose Lundy Virginia Sterling UK Hemel Hempstead2 Thailand Bangna Malaysia Cyberjaya3 Australia Sydney1	172.22.0.0/17 172.22.128.0/17 10.223.0.0/17 10.223.128.0/17
Frankfult 2 Data Center	172.22.0.0/16 10.223.0.0/16

- If you use the Internet Connectivity and VPN Connectivity in combination, direct back and forth communication between the Internet and VPN via vFirewall or Integrated Network Appliance will not be possible.
- If you started using the VPN Connectivity at Yokohama No.1 Data Center on or before November 15, 2013 and have not carried out lease construction for changing bandwidth, you should pay attention to the following points.

✧ To be Customer Portal available

- VPN Connectivity service termination and new order is needed.

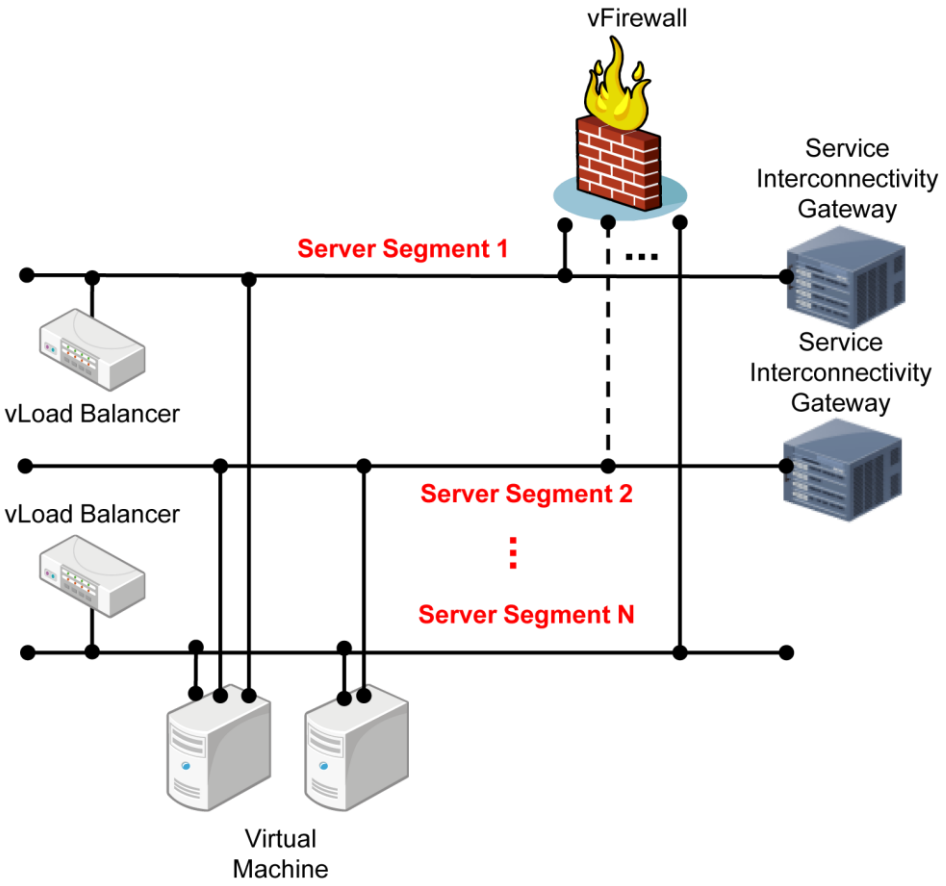
- ✧ Change bandwidth
  - Lease construction is necessary for changing bandwidth. Please specify a construction date of at least 17 business days after the date you order it. Also, on the date of construction there might be multiple communication interruptions that last up to several tens of minutes each.
  - If you are connected to a VPN other than Arcstar Universal One Service when the above-mentioned leased construction takes place, you will need to transfer to Arcstar Universal One.
  - Prefix Length of IP Address Blocks /29-/8 are availeable.

- If you started using the VPN Connectivity at Yokohama No.1 Data Center after November 15, 2013, you should pay attention to the following points.
  - ✧ To be Custome Portal Available
    - VPN Connectivity service termination and new order is needed.
  - ✧ Change bandwidth in order form
    - Lease construction is not necessary. 17 business days is needed to change.
- APGW Connectivity segment setting is not necessary in Customer Portal available VPN Conectivity. And 1Gbps Guaranteed plan is not available.

5.3 Server Segment

Server segment is a service that extends Server Segments. We provide L2 segments (called "Server Segment" below) to interconnect the multiple services that make up Enterprise Cloud.

You can connect the Virtual Machines, vLoad Balancers and Service Interconnect Gateways over the Server Segment and also construct systems with complex network structures.



INFO ● The standard is for one Server Segment to be provided

5.3.1 Available Features

The following features are available for Server Segment.

Feature	Overview
Server Segments are provided	A feature that uses L2 segments to interconnect the multiple services which make up Enterprise Cloud.

5.3.2 Server Segments Are Provided

The standard is for two Server Segments to be provided. You can specify Server Segments within the ranges listed below for each Data Center.

Server Segment	Lower Limit	Upper Limit	Setting Unit
When using vFirewall	1	24	1
When using Integrated Network Appliances	1	24※	1

※ Maximum Server Segments which can connect to INA are up to 7.

Features that can be Interconnected

The following features can be connected using Server Segment.

- Virtual machines provided by Compute Resource
- Virtual machines provided by Compute Resource (Dedicated Device)
- vFirewall that is provided by vFirewall
- vLoad Balancer that is provided by vLoad Balancer
- Service Interconnect Gateway that is provided by Service Interconnectivity
- Colocation Interconnectivity
- Gateway provided by On-Premises Interconnectivity

Settings When Adding Server Segment

When you ask for Server Segment, you must specify the following settings.

Item	Overview
Network Appliance	Specify whether or not to connect to vFirewall or Integrated Network Appliance.
IP address block for Server Segment	For each Server Segment, you can allocate one IP address block for Server Segment and a prefix length of IP address blocks (any of /29 to /24).

NOTE

- You cannot change whether or not to connect to vFirewall or Integrated Network Appliance and the IP address block for Server Segment after the Server Segment has been created.
- If you do not connect the Server Segment to vFirewall, NTT Communications cannot perform Ping monitoring on any device connected to that Server Segment.

Types of IP Address Blocks

The IP address blocks used for Server Segment are divided into the following categories. Please check the explanation of the features of each service for the connection interfaces.

Category	Overview
Available IP address	IP addresses that can be allocated to interfaces that connect to a Server Segment
Allocated IP address	IP addresses that have been allocated to interfaces that connect to a Server Segment
Reserved IP address	IP addresses that cannot be allocated to interfaces that connect to a Server Segment ※ These are excluded from the candidates for allocation when IP addresses are allocated automatically by the system or they are allocated at your discretion. Reserved IP addresses are set by the Customer Portal.

Setting DNS and Default Gateway IP Addresses

You can specify the following Parameters when creating Server Segment. This setting is referenced when the Virtual Machine is created (and when vNIC is reconstructed), and each IP address that is set for the Server Segment that is the connection destination for Primary vNIC is given the initial settings by the Guest OS of the Virtual Machine.

- DNS Server (Primary DNS and Secondary DNS) IP addresses
- Default gateway IP addresses
- DNS suffix

The parameter setting for each address differs depending on whether customer uses vFirewall or Integrated Network Appliance.

	vFirewall	Integrated Network Appliance
DNS Server (Primary DNS, Secondary DNS) IP Address	・IP addresses specified by Customer or NTTCommunications	
Default gateway IP Address	・Customer can specify the IP address at the time Server Segment is created. (Cannot be changed after activation) If it was not specified vFirewall AcitveIP address is	・When the segment is connected to INA, ActiveIP address is assigned. It cannot be changed. ・When the segment is not connected to INA, Customer can specify the IP address.It cannot be changed. When the IP address is not be specified NTT Communications will be

	assigned.	specified.
DNS suffix	・IP addresses specified by Customer or no value	

※ The IP address that is set for Server Segments that do not connect to the Integrated Network Appliance is "the "broadcast address" of the IP address block for the Server Segment - 1." For example, if the IP address block is "192.168.0.0/24," the IP address that is "the "broadcast address" of the IP address block for the Server Segment - 1" will be "192.168.0.254."

- You can only specify the DNS and default gateway IP address at the time Server Segment is created.

  If IP addresses have not been specified, they will be allocated automatically as shown below.

Service	Allocatable IP Addresses
DNS Server（Primary DNS、Secondary DNS）	IP addresses specified by NTT Communications
Default Gateway	When connected to vFirewall or Integrated Network Appliance : Active IP Address of each Network Appliance When not connected to vFirewall or Integrated Network Appliance: IP address specified by NTT Communications

- Restrictions in case of default GW is specified by Customer

  vFirewall:The IP address which is set as a Default Gateway cannot be assigned to the vNIC of the Virtual Machine.

  INA:The IP address which is set as a Default Gateway cannot be assigned to the vNIC of the Virtual Machine and Service Interconnectivity Gateway.

※ DNS IP address auto assigned by Guest OS Custmization is not available for resolver. It is dummy IP address. Customer prepare DNS, please.

5.3.3 Important Points

- To add, delete, or set a Server Segment, you must submit an application form in Germany Frankfurt2 Data Center.
- The one Server Segment that is provided as standard when you start using the Data Center are always connected to vFirewall or Integrated Network Appliance.
- Server Segment cannot be deleted as long as the templete exist on Private Catalog, when Virtual Machine which vNIC connecting the Server Segment is converted.
- The IP Addresses in the IP Address bands listed below cannot be specified as IP address blocks for Server Segments. Be aware that the IP address bands that cannot be specified differ according to Data Center.

Data Center	Non-duplicatable IP Address Bands
Yokohama No.1	172.22.0.0/17 172.22.128.0/17 10.223.0.0/17 10.223.128.0/17
Kansai 1	172.23.0.0/17 10.233.0.0/17 172.23.128.0/17 10.233.128.0/17
Saitama No.1	172.27.0.0/16 10.237.0.0/16 10.238.0.0/16
Hong Kong Tai Po	172.22.128.0/17 172.31.128.0/17 10.223.128.0/17 10.224.128.0/17
Singapore Serangoon	172.20.0.0/17 10.200.0.0/17 172.20.128.0/17 10.200.128.0/17
San Jose Lundy Virginia Sterling UK Hemel Hempstead2 Thailand Bangna Malaysia Cyberjaya3 Australia Sydney1	172.22.0.0/17 172.22.128.0/17 10.223.0.0/17 10.223.128.0/17
Frankfult 2 Data Center	172.22.0.0/16 10.223.0.0/16

- Customer’s carried-in Global IP Address can be assigned to Server Segment.

However, please note that there are folowing restrictions.

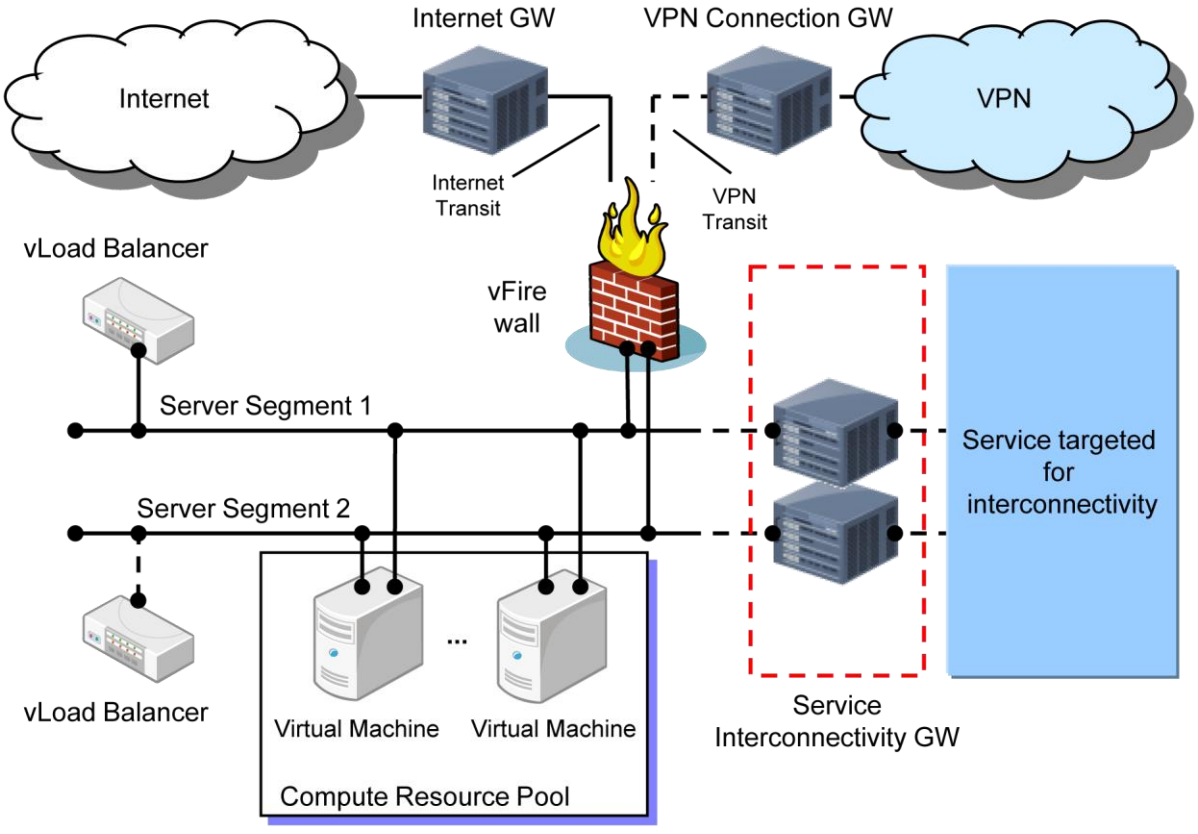
- Please apply via Service Order Form when adding Server Segment with Customer's carried-in Global IP Address.

- The direct Internet transmission is not possible via vFirewall or Integrated Network Appliance when using the Customer's carried-in Global IP Address. NAT setting is necessary for the Global IP Address provided by NTT Communications.

- If the registered name for IP Address under NIC orgnization and the representative contractor name of Enterprise Cloud service does not match, the carried-in IP address would be considered as illegal Global IP Address and it cannot be supported. Also, we cannot guarantee the sustainability of the carried-in Global IP Address.

5.4 Service Interconnectivity

Service Interconnectivity provides a Service Interconnect Gateway (called "Service Interconnect Gateway" below), which connects services targeted for interconnectivity, such as Server Segment and Global File Storage (Global Data Backup) that are used for Enterprise Cloud. Note that at the Japan Data Centers you can also connect to Network Storage Service and systems inside colocation, etc.



5.4.1 Available Features

You can use the following features in Service Interconnectivity.

Feature	Overview

Service Interconnect Gateway	A feature that uses L3 connectivity to interconnect Server Segments used for Enterprise Cloud and services targeted for interconnectivity.
Routing Settings	A feature that sets static routing between the Server Segments used for Enterprise Cloud and services targeted for interconnectivity.

5.4.2 Service Interconnect Gateway

The Service Interconnect Gateway operates as a router. Using an L3 connection, it connects Server Segments used for Enterprise Cloud and the networks used by services targeted for interconnectivity.

You can specify the number of Service Interconnect Gateway that can be used in the same Data Center within the range listed below.

	Lower Limit	Upper Limit	Units Provided
Service Interconnect Gateway	1	The number of Server Segments in use (※maximum 24 units)	1

※ With Service Interconnectivity, you can install one Service Interconnect Gateway for each Server Segment.

NOTE

- You can select the IP addresses used for Service Interconnectivity from the available IP Addresses. You can only specify them at the time the Service Interconnect Gateway is created based on the application form.

  If IP addresses have not been specified, they will be allocated automatically.
- You cannot change the IP addresses that are used for Service Interconnectivity after you have started using Service Interconnectivity.

INFO

- The Service Interconnect Gateway is configured in an active/standby structure, so one virtual IP, one active device IP and one standby device IP address are used.
- The Service Interconnect Gateway is a Best Effort type service that changes the transmission speed according to your system environment and line congestion.

5.4.3 Routing Settings

You can set a maximum of 32 types of static routing for Service Interconnect Gateway, including the default gateway.

INFO

- The static routing settings are implemented based on parameter sheets agreed upon with you and the policies of NTT Communications.

5.4.4 Important Points

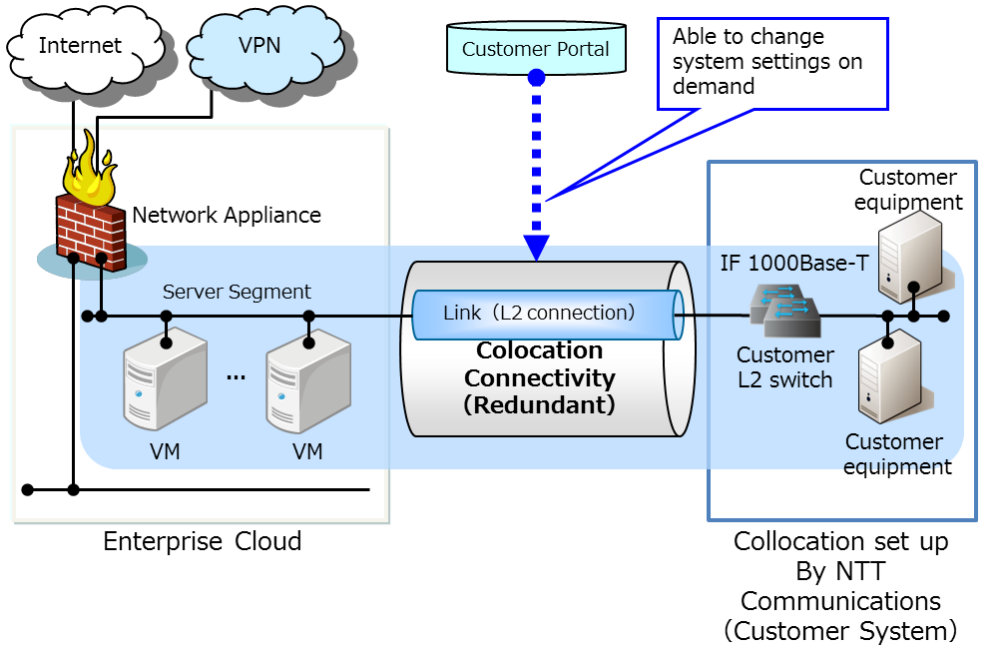
- When using the same Server Segment Service Interconnectivity from a Virtual Machine that has the default gateway set as vFirewall, the routing information of the

service targeted for the Service Interconnectivity side must be set to the Guest OS on the Virtual Machine.

- Please refer to the explanation about services targeted for interconnectivity regarding the requirements for connection with these services.

5.5 Colocation Interconnectivity

Colocation Interconnectivity is a service that provides a secure L2 connection between the Server Segment that NTT Communications provides and your system environment inside our colocation via our inter-Data Center network.



5.5.1 Available Features

You can use the following features in Colocation Interconnectivity.

Feature	Overview
Layer 2 (L2) Connection	A feature that connects the Server Segment NTT Communications provides and your system environment inside our colocation using the same Server Segment.

5.5.2 Layer 2 (L2) Connection

For one colocation connection, you can have L2 connections with Server segments (a maximum of 24 Server Segments) using tagging VLAN.

INFO

- The colocation connection is constructed of redundant physical devices (equipment and lines).
- The maximum bandwidth that can be used by one colocation is 1 Gbps.

  After starting use, you can start/stop using the service by changing the communication bandwidth settings (1000Mbps/0 Mbps), and add/delete VLAN from the Customer Portal.

Connectable Colocations

The colocations that can be connected differ according to Enterprise Cloud Service Data Center. The following are the colocations that can be connected.

Enterprise Cloud Service Data Center	Destination Colocation Data Center
Yokohama No. 1	Yokohama No. 1, Tokyo No.2 and Tokyo No.3 Tokyo No. 5 and Tokyo No. 6 and Saitama No.1
Kansai 1	Kansai 1 Data Center and Osaka (Dojima) No. 1, 2 and 3,Kyoto No.2
Saitama No.1	Yokohama No.1, Tokyo No.2, Tokyo No.3 , Tokyo No.5, Tokyo No.6 and Saitama No.1

INFO

- You can connect to multiple colocations at each Enterprise Cloud Service Data Center.

Networking

According to the rack location that you specify, any of the following methods will be provided after the facility is studied by NTT Communications. You cannot select the method to be provided.

- UTP x 2 units
- Media Converter x 2 units

  The media converter specifications are shown below (specifications of Japan Data Center).

  Contact us for specifications of overseas Data Center.

Item	Details
Height x Width x Depth	4.24 cm × 13 cm × 20 cm
Weight	0.7 kg or less (including AC adapter)
Power supply type	AC100 V
Power consumption (AC adapter)	10 W or less
Power redundancy	Single
Connection wiring	MDI-X
Linkdown forwarding	Yes

NOTE

- You must prepare a separate location and power supply for the media converter.
- In order to connect the media converter, you must have two Ethernet cables with the same rating that are Enhanced Category 5 (Cat 5e) or greater.

Customer L2 Switch

Please be aware of the following points regarding the Customer L2 switch settings.

- For one colocation connection, a maximum of 24 VLANs can be used. Please connect the Customer L2 switch VLAN port using tagged settings. The range of VLAN IDs where you can specify is from 2 to 4094. The maximum number of steps of a VLAN tag is one step.
- Priority control cannot be performed according to CoS values.
- Please set Interface as 1000GASE-T, the connection procedure to Auto Negotiation.
- The UTP x 2 cables and the media converter x 2 units, which are the connection points, have a redundant configuration. Please set L2 switch as active and standby configuration to avoid frame a loop in Layer 2 and connection braking off.
- Please set the Customer system so that no problems occur if part of the provided network has a communication interruption.
- The minimum frame length is 68 bytes (tag) and the maximum is 1,522 bytes (tag).
- IEEE 802.3x (pause) and LLDP cannot be used with the Customer L2 switch.

NOTE

- To set redundant configuration customer selected, please use the VLAN-ID between from 2 to 4094 with tagged settings. Please confirm beforehand wheater the L2 switch prepared for this service can be available to use tagged settings.
- The checking-of-operations protocol used by Cisco is as follows.
  - PVST+ and Rapid PVST+ and Flex Link [IOS 12.2(53)SE2] (NTT Communications does not support about actual connectivity in all IOS version.)
- Untagged control frame defined by Spanning Tree Protocol (IEEE 802.1d) will be discarded systematically.

INFO

- L2 Broadcast, L2 Multicast and Unknown Unicast that exceed 10 Mbps may be discarded.

  Even if the communication bandwidth is set to Disabled (0 Mbps), the control frames can communicate at approximately 100kbps and other frames can communicate at a few kbps.

5.5.3 Important Points

- Please set acitive and standby redundant configuration in Customer L2 switch interface.
- Communication cutting by operation of a Cusotmer's redundant control becomes the outside of SLA.
- If a failure occurs on the communication path of this service, the communication path is automatically switched to another route and communications are restored in approximately 30 seconds.
- Within the Customer system environment that is connected by colocation interconnectivity, one MAC address can be used for one IP address.
- The MAC addresses used by Enterprise Cloud are shown below. For the Customer system, please use MAC addresses that do not duplicate the following MAC addresses.

  Note that the following MAC addresses may be changed. We apologize in advance for this.

  - MAC addresses that begin with 00-50-56 (VMWare)
  - MAC addresses that begin with a2
  - MAC addresses that begin with 00-0b-fc-fe-1b
  - MAC addresses that begin with 00-00-0c-07-ac
  - 00-00-0c-9f-f0-00～00-00-0c-9f-ff-9f (※1)
  - 00-00-5e-00-01-00～00-00-5e-00-01-fb (※2)
- Multiple Links (two or more contracts) can be increased connection bandwidth between Enterprise Cloud and Colocation. But one Server Segment can be connected to one link.

  ※1 Please use from 00-00-0c-9f-ff-a0 onward for the Customer system.

  ※2 Please use from 00-00-5e-00-01-fc onward for the Customer system.

5.6 On-Premises Interonnectivity

On-Premises Interconnectivity is a service that provides a secure L2 connection between the Server Segment NTT Communications provides and your system environment inside the environment that you operate yourself (called, "On-Premises Environment" below), via the Internet. For On-Premises Interconnectivity, the On-Premises GW is installed in the Data Center and the On-Premises Environment.

INFO
- The On-Premises Interconnectivity gateway is constructed of redundant physical devices.

5.6.1 Available Features

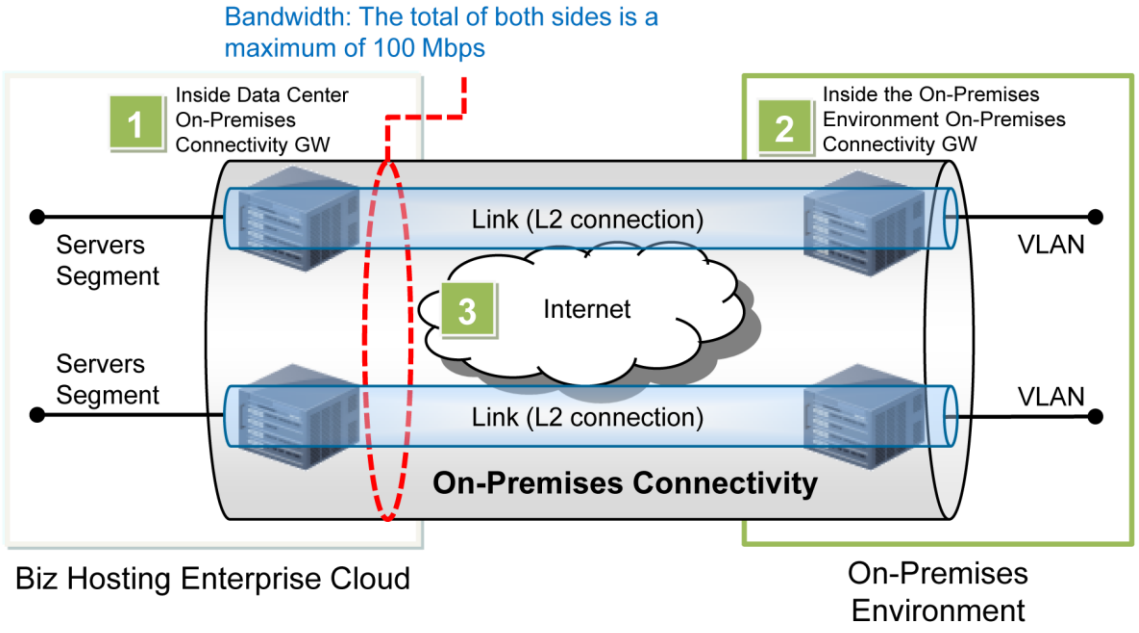
You can use the following features in On-Premises Interconnectivity.

Feature	Overview
Layer 2 (L2) Connection	A feature that connects the Server Segment NTT Communications provides and the On-Premises Environment using the same Server Segment.

5.6.2 Layer 2 (L2) Connection

On-Premises Interconnectivity is composed of the following devices.

1	On-Premises GW inside the Data Center
2	On-Premises GW inside the On-Premises Environment
3	Connected network (Internet)



Adding and Reducing L2 Connections

You can add, change and delete L2 connections between NTT Communications's Server Segments and On-Premises Environment, within the ranges listed below for one On-Premises Interconnectivity.

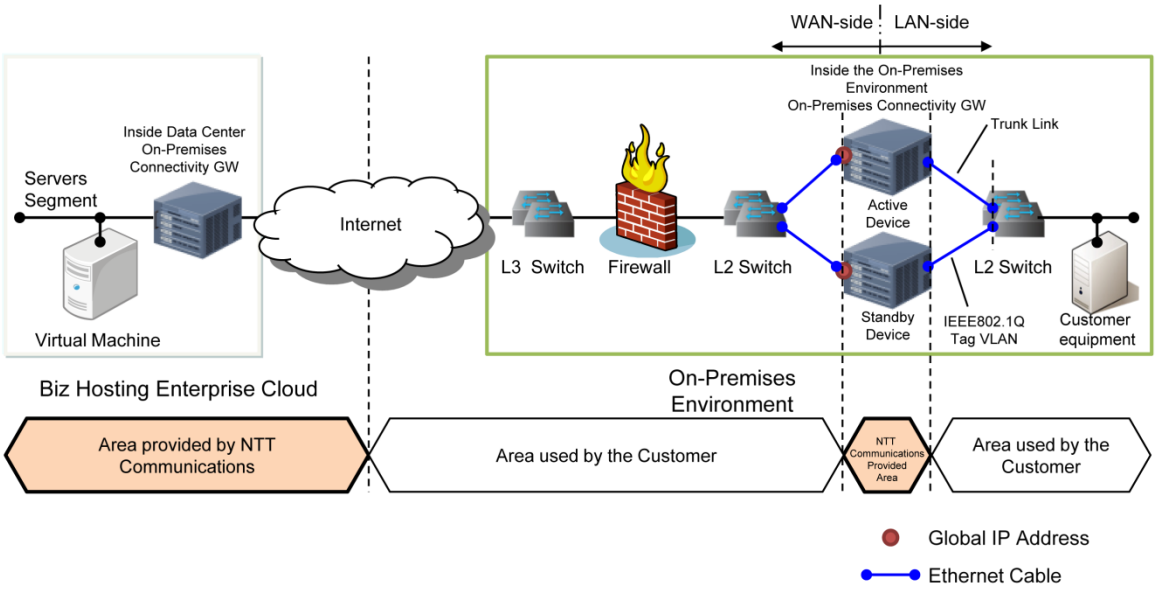
	Lower Limit	Upper Limit	Setting Unit
Number of L2 connections	1	24	1

INFO

- You can connect to multiple On-Premises Environments at each Data Center.
- The bandwidth that can be used for one On-Premises Interconnectivity is a maximum of 100 Mbps for the total communication going both ways.
- The connection network is provided via the Internet, so quality cannot be guaranteed.

Use Conditions for On-Premises Interconnectivity

The following shows an example of general On-Premises Environment structure. Here is an explanation of the required conditions for the On-Premises Environment, for connecting between Server Segment and the On-Premises Environment.



NOTE

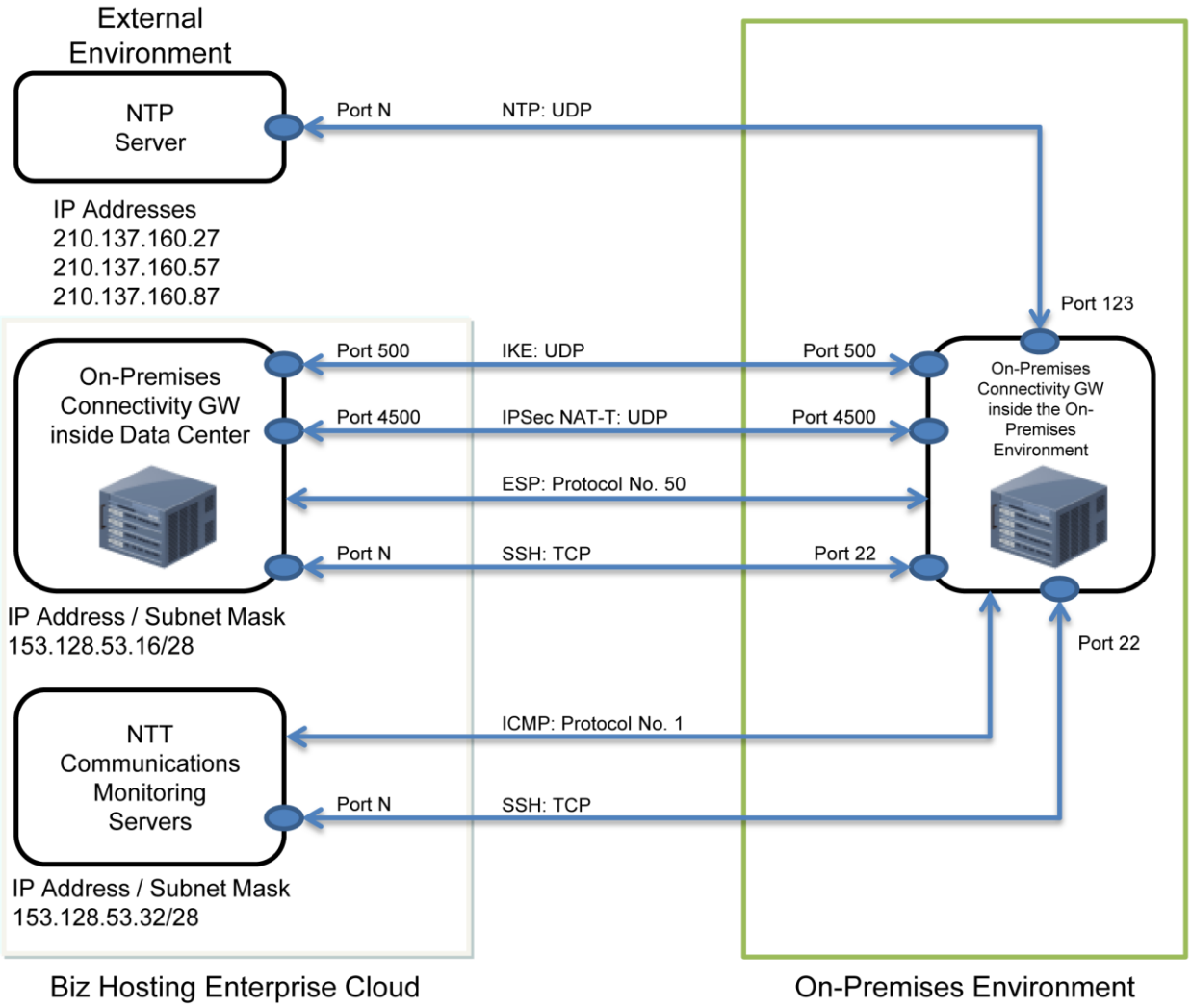
- You are responsible for the design and settings of "your own area" within the On-Premises Environment.

On-Premises GW inside the Data Center

- The connection line from the On-Premises GW inside the Data Center to the Internet is provided by dedicated On-Premises Interconnectivity lines. An Internet Connectivity service is not necessary. For details on Internet Connectivity, refer to "5
- Internet Connectivity" (⇒P.130).

Between the devices inside the Data Center and the On-Premises GW inside the On-Premises Environment

- The communication infrastructure that is used for the On-Premises Interconnectivity between the devices inside the Data Center and the On-Premises GW inside the On-Premises Environment is shown below.



- We recommend using a firewall to connect securely to the Internet. You need to set up your own firewalls. Please allow the following protocol communication in order to implement On-Premises Interconnectivity.

Purpose	Protocol No.	Source IP Address	Destination IP Address	Source Port	Dest. Port
NTP	17(UDP)	Global IP Address (※)	210.137.160.27 210.137.160.57 210.137.160.87	-	123
		210.137.160.27 210.137.160.57 210.137.160.87	Global IP Address (※)	123	-

IKE	17(UDP)	Global IP Address (※)	153.128.53.16/28	500	500
		153.128.53.16/28	Global IP Address (※)	500	500
SSH	6 (TCP)	Global IP Address (※)	153.128.53.16/28 153.128.53.32/28	22	-
		153.128.53.16/28 153.128.53.32/28	Global IP Address (※)	N	22
ESP	50	Global IP Address (※)	153.128.53.16/28	-	-
		153.128.53.16/28	Global IP Address (※)	-	-
ICMP	1	Global IP Address (※)	153.128.53.16/28	-	-
		153.128.53.32/28	Global IP Address (※)	-	-

※ This is a Global IP Address allocated to the On-Premises GW inside the On-Premises Environment.

On-Premises GW inside the On-Premises Environment

- There must be four Ethernet cables with the same rating of Category 5 (Cat 5) or greater.
- For each On-Premises Interconnectivity, two physical servers are set up which have the virtual appliances provided by NTT Communications (Active Device: one unit and Standby Device: one unit), as On-Premises Connection GW inside the On-Premises Environment.
- The specifications for physical servers for the On-Premises Connection GW inside the On-Premises Environment are shown below. An air-conditioned environment is required to keep the racks and power supplies that can be used under these conditions at a suitable humidity and temperature.

Item	Details
Height x Width x Depth	8.59 cm × 44.54 cm × 69.98 cm
Weight	20.41 kg (minimum) to 27.22 kg (maximum)
Number of racks required	19-inch rack, 2U
Rack rail requirements	Slide-type universal rack rails with adjustable length (61-91 cm) to fit square hole and round hole cabinets
Number of electrical connections	1 (redundancy not possible)

Power supply requirements	1,200 W
Networking interface requirements	100Base-TX、1000Base-T
Temperature conditions	10 to 35°C
Height conditions	0 to 3,050 m
Humidity conditions	10 to 90% and no condensation

On-Premises GW inside the On-Premises Environment (WAN side)

- It is necessary to have a connection line to the Internet that can be used from the On-Premises Environment.
- There must be two Global IP Addresses (fixed) that can be used for a connection line to the Internet that can be used from the On-Premises Environment.

  The Global IP Addresses are allocated to the interface for the On-Premises GW inside the On-Premises Environment. They are used for communication with the devices inside NTT Communications's Data Centers and NTP servers.

On-Premises GW inside the On-Premises Environment (LAN side)

- Please connect the On-Premises GW inside the On-Premises Environment (LAN side) to an L2 switch (trunk link) that uses a tag VLAN that is regulated by IEEE802.1Q.
- The VLAN ID (Identification Number) used must fulfill the following conditions.

Usable VLAN ID Range	2 to 4,094
Number of VLAN IDs required for Server Segment connection	1 to 24
VLAN ID (※) used in redundant configuration	1
Number of MAC addresses for each connected Server Segment	The number that can be used differs depending on the prefix length. ● For /26: 60 ● For /25: 124 ● For /24: 252

※ For the redundant VLAN ID, please specify a VLAN ID that is smaller than the number of the VLAN that is used for On-Premises Interconnectivity. For example, if the VLAN ID that is used for the L2 connection inside the On-Premises Environment has the number 500, specify numbers from 499 and below for the redundant VLAN ID.

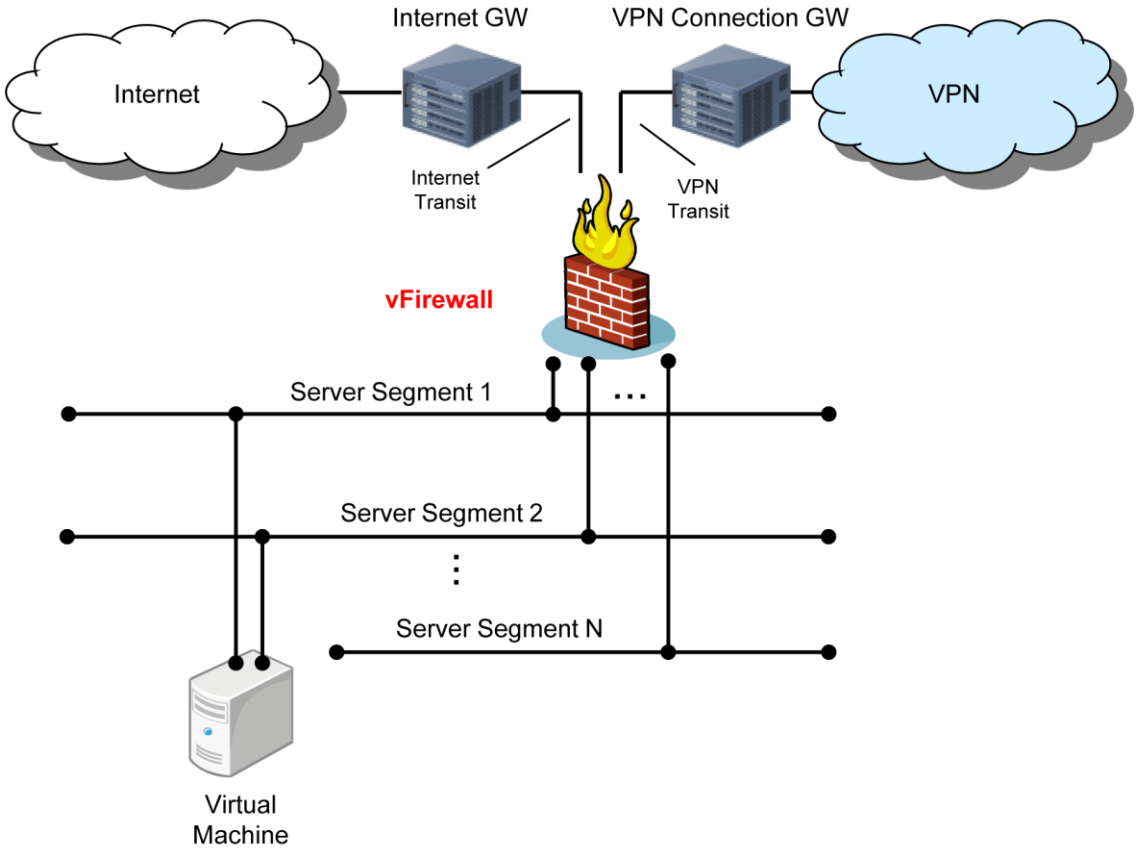
5.6.3 Important Points

- If failures occur, the switchover from the active device to the standby device will be performed automatically. The time taken from when the reason for the switchover occurs to when the switchover is completed is generally just a few seconds. Even when the failure in the active device is solved, it does not switch over to the active device.
- Within the On-Premises Environment, the NTT Communications is only responsible for the On-Premises GW.
- On-Premises GW inside the On-Premises Environment can only be installed (address) inside Japan. They cannot be installed outside of Japan.
- If failures caused by your deliberate act occur to the physical server owned by NTT Communications that features as the On-Premises GW inside the On-Premises Environment, you may be held responsible for restoring it to its original condition.
- You cannot use an NAT feature using a network device for the connection from On-Premises GW inside the On-Premises Environment to the Internet.
- You cannot use one Server Segment for multiple L2 connections.
- You cannot connect multiple VLANs set inside a single On-Premises Environment to the same Server Segment simultaneously.
- To add and use a VLAN ID that is lower than the redundant VLAN ID in the L2 tunnel, you need to change the redundant VLAN ID.
- If different IP address blocks or subnet masks are set for the Server Segments and VLAN inside the On-Premises Environment that connect via L2, NTT Communications assumes no responsibility whatsoever for issues arising from those settings.
- You are responsible for IP address design in the On-Premises Environment and Enterprise Cloud. NTT Communications assumes no responsibility for any failures that may occur due to IP design problems.
- In order to prevent adverse effects on shared equipment, NTT Communications uses settings that partially restrict multicast and broadcast communications.
- If the MAC address of the Virtual Machine of Enterprise Cloud and the MAC address of the devices inside the On-Premises Environment overlap, the Customer might be required to change the MAC addresses. Also, if MAC addresses adversely affect equipment shared with other customers, we might restrict the use of On-Premises connection without prior permission from you.

5.7 vFirewall

vFirewall is a service that, as a firewall feature, mainly provides routing, packet filtering, and NAT/NAPT features. vFirewall provides you with a dedicated vFirewall.

You can change parameters from the Customer Portal.



NOTE

- When you start using vFirewall, it reads the packets that pass through the vFirewall, judges the contents, and dynamically opens and closes the ports. It is effective as a stateful packet inspection feature that blocks unauthorized access.

  You cannot disable this feature.

INFO

- It is absolutely necessary to have a contract for either vFirewall or Integrated Network Appliance for one Enterprise Cloud Service. However, customer cannot have a contract for both.
- vFirewall can connect to the Internet, VPN, and Server Segment.
- vFirewall is constructed of redundant physical devices (equipment and lines).

5.7.1 Available Features

You can use the following features in vFirewall.

Feature	Overview
Routing Feature	A feature that connects to Internet Transit, VPN Transit and Server Segment, and performs the routing among them.
Firewall Feature	A feature that provides a dedicated vFirewall to the Customer inside the environment provided by Enterprise Cloud.
Packet Filtering Feature	A feature that sets whether IP communication is allowed or denied, among the routings that can be used by the routing feature.
NAT/NAPT Feature	A feature that translates IP addresses and ports among Internet Transit, VPN Transit and Server Segment.

vFirewall IP Addresses

The IP addresses used by vFirewall are shown below.

Device	Allocatable IP Addresses
Internet Transit	Selected from Global IP Addresses that are ordered separately
VPN Transit	Selected from your VPN IP Address block (called "IP address block for VPN transit" below)
vFirewall	NTT Communications selects two IP addresses from the IP address block for VPN transit (※)
Virtual Network Interface for connecting to a Server Segment (called the "network interface on the Server Segment-side" below)	Two are selected from the available IP addresses in Server Segment. (※)

※ Because it is configured in an active/standby structure, an active device uses one IP Address and a standby device uses one IP Address.

NOTE

- You can specify the IP address on the Server Segment-side network interface only when the Server Segment is created based on the application form.

  If IP addresses have not been specified, they will be allocated automatically.
- You cannot change the IP addresses that are allocated to the Server Segment-side network interface.

INFO

- If you do not configure Server Segment-side network interface, the corresponding Server Segments will not be connected with vFirewall. If you do not connect the Server Segment to vFirewall, NTT Communications cannot perform Ping monitoring on any device connected to that Server Segment.

5.7.2 Routing Feature

When Internet Connectivity and VPN Connectivity are in use, vFirewall will be connected with each network and Server Segment.

This feature performs routing between each network and Server Segment.

Static Routing

You can also set static routing to the vFirewall.

For each routing setting, the routing conditions that can be set are shown below.

- Network Address
- Gateway
- Output Interface

INFO

- If you use Internet Connectivity and VPN Connectivity in combination, direct back and forth communication between the Internet and VPN via vFirewall will not be possible.
- The routing that uses the same interface for input interface and output interface is not possible.

5.7.3 Firewall Feature

You can specify the performance provided by vFirewall using the vFirewall resource value.

The performance of one vFirewall resource is shown below. You can change the resource value from the Customer Portal.

Item	Performance (maximum value)	Remarks
Traffic Processing Capacity	40 Mbps	The processing capacity for transferring IP packets received into vFirewall (incoming packets from vLoad Balancer are excluded)
Number of concurrent sessions	10,000	The number of TCP/UDP sessions that can be held simultaneously inside vFirewall
Number of filter rule settings	30	-

Number of IP address group settings	5	If there is one vFirewall resource, the maximum value is 10. If vFirewall resources have been added, the maximum value for "Number of IP Address Group Settings" for the additional vFirewall resource is 5.
Number of service group settings	5	If there is one vFirewall resource, the maximum value is 10. If vFirewall resources have been added, the maximum value for "Number of Service Groups" for the additional vFirewall resource is 5.
Number of routing settings	5	-

IP Address Group Settings and Service Group Settings

In order to improve the convenience of setting vFirewall from the Customer Portal, features to set IP address groups and service groups are provided.

Item	Overview
IP address group settings	You can group IP addresses. The set IP Address Group can be used for, Packet Filtering setting.
Service group settings	You can group TCP/UDP ports and ICMP Types. You can use the set service groups with packet filtering settings.

Adding and Reducing vFirewall Resources

You can add and reduce usable vFirewall resources, within the following range.

	Lower Limit	Upper Limit	Application Unit
vFirewall resources	1	50 (※)	1

※ The maximum value that can be set using the Customer Portal is 10. Please contact us separately if you would like 11 or more vFirewall resources.

5.7.4 Packet Filtering Feature

A feature that specifies IP Packet filter conditions (packet filtering policy) for vFirewall. It can allow or deny the passage of IP packets that match the filter conditions.

You can specify the following conditions for each filter rule as IP packet filter conditions to apply to packet filtering.

Item	Overview
Interface	Select any of the following as the network interface of vFirewall that implements packet filtering. ● Internet Transit ● VPN Transit ● Server Segment
Source IP Address	Specifies a source IP address or IP address group for IP packets.
Source Service	Specifies the TCP/UDP ports, ICMP type, or service group as the source service for IP packets.
Destination IP Address	Specifies a destination IP address or IP address group for IP packets.
Destination Service	Specifies the TCP/UDP ports, ICMP type, or service group as the destination service for IP packets.
Actions	Specifies whether to allow or deny the passage of IP packets that match the conditions set by the above-mentioned items.

NOTE

- Even if you start using vFirewall, filter rules will not be set automatically. In this case, all packets will be denied. In order to allow communication, after starting to use vFirewall, please set filter rules at your discretion from the Customer Portal.

5.7.5 NAT/NAPT Feature

For vFirewall, you can set IP Address Translation and IP Address Port Translation (called "NAT/NAPT" below) rules between Internet Transit, VPN Transit and Server Segment.

The maximum number of NAT/NAPT setting rules that can be set for a single vFirewall is 256.

INFO

- You can translate IP addresses either 1 to 1 or 1 to N.
- The IP addresses that can be set to NAT/NAPT differ depending on the network that executes NAT/NAPT.

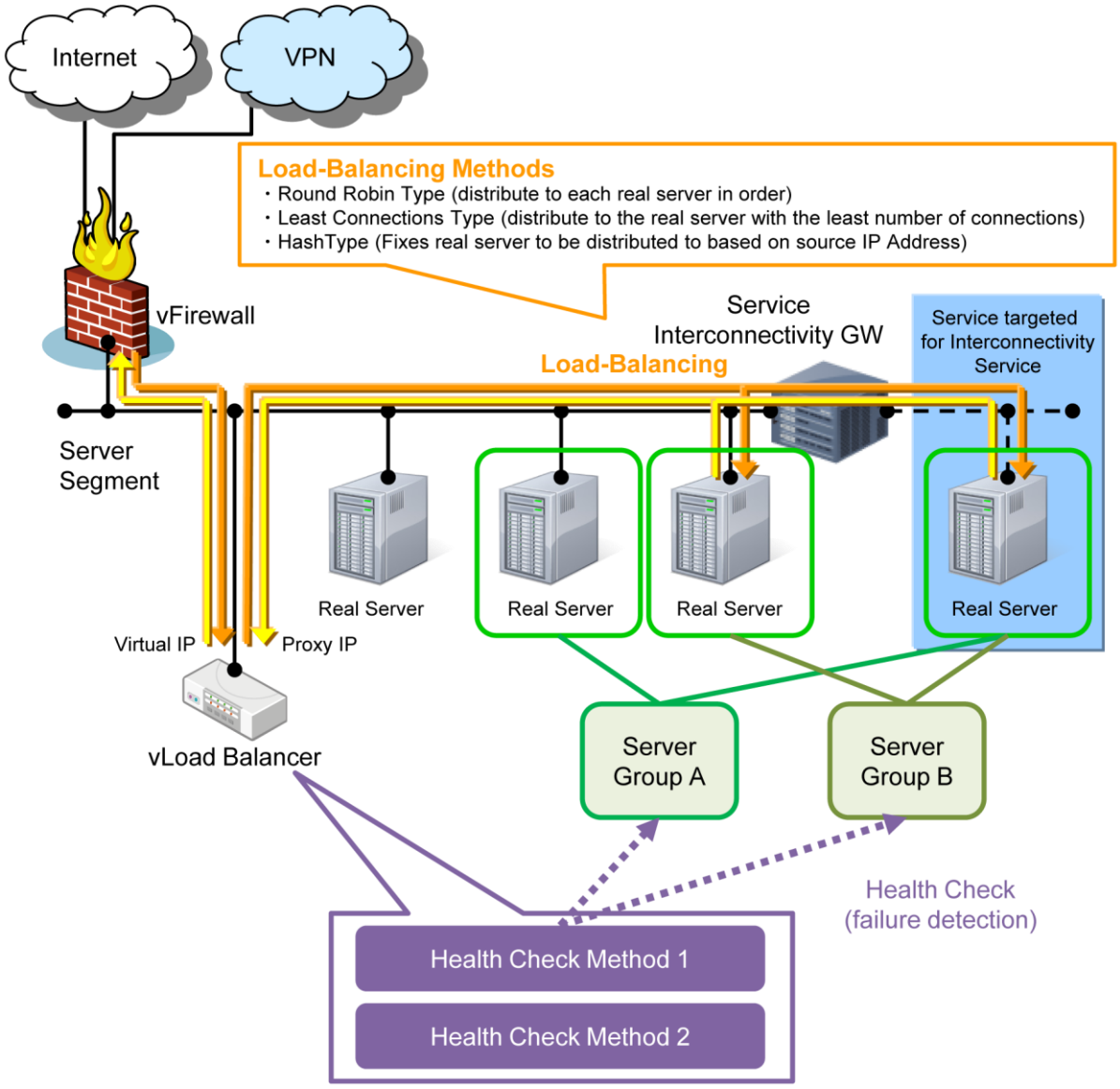
Network Type	Allocatable IP Addresses
Internet Transit	Global IP Address that is used for Internet Connectivity
VPN Transit	For VPN Connectivity, an unused IP address from the IP address block that is allocated to VPN Transit
Server Segment	Any IP address

5.7.6 Important Points

- NTT Communications may change vFirewall settings in order to perform maintenance and monitoring. You cannot change or delete the settings that are set by NTT Communications.
- Communication interruptions might occur when you change vFirewall settings from the Customer Portal.

5.8 vLoad Balancer

vLoad Balancer is a service that provides a virtual dedicated load balancing device over the Server Segment. You can use the load balancing feature for communication with Virtual Machines in a Server Segment.



5.8.1 Available Features

You can use the following features in vLoad Balancer.

Feature	Overview
Load Balancing Feature	A feature that balances the communication load for the Virtual Machine on the Server Segment.
Routing Feature	A feature that sets static routing to vLoad Balancer.
IP Address Delivery Feature	A feature that provides a Virtual IP (called "VIP" below) for communication between vLoad Balancer and vFirewall, and a feature that provides a Proxy IP for communication between vLoad Balancer and the load balancing destination server (called "real server" below).

INFO
- You can install one vLoad Balancer unit to each Server Segment.
- You can change the settings of vLoad Balancer from the Customer Portal.

5.8.2 Load Balancing Feature

vLoad Balancer Performance

You can specify the performance provided by vLoad Balancer using the vLoad Balancer values.

The performance of one vLoad Balancer resource is shown below.

Item	Performance (maximum value)	Remarks
Traffic Processing Capacity	20 Mbps	Processing capacity for transferring IP packets received into vLoad Balancer
Number of concurrent sessions	20,000	Number of TCP/UDP sessions that can be held simultaneously inside vLoad Balancer. ※ Unlike vFirewall, when inbound and outbound communications occur, each one session is held.
Number of Health Check Definitions	10	-
Number of Real Server Settings	20	-
Number of Server Farm	20	-

Settings		
Number of VIP Settings	4	-
Number of routing settings	5	-

Adding and Reducing vLoad Balancer Resources

You can add and reduce usable vLoad Balancer resource values, within the following range.

	Lower Limit	Upper Limit	Application Unit
vLoad Balancer Resource Value	1	50 (※)	1

※ The maximum value that can be set using the Customer Portal is 10. Please contact us separately if you would like 11 or more vLoad Balancer resources.

Load-Balancing Features

In order to perform load balancing, you can set load-balancing rules that specify targeted server, health check method and load-balancing method. You can set the following items for each load-balancing rule. See the User Guide for the setting method.

Setting Name	Setting Details
VIP	From the VIP provided to the vLoad Balancer, specify the VIP to use for load-balancing rules.
Protocol	Selects the protocol of communication to be load-balanced from TCP or UDP.
Port	Specifies the port number of communication to be load-balanced.
Session Maintenance Method	Selects the method for maintaining sessions. ● Source IP Address Method ● Cookie Insert Method (available only for HTTP communication)※ – Cookie header insert (Expiry of the cookie) “Yes” until browser discards cookie “No” timeout in 60 seconds
Server Group	Specifies the server groups to which to apply these load-balancing rules. ● Selects the health check method from any one of the following. – TCP Port

	– ICMP Ping ● Selects the load-balancing method from any one of the following. – Round Robin (Distributes to each real server (load balancing destination server) in order) – Hash (Fixes the real server that is distribution destination based on the hash value of the source IP address) – Least Connections (Distributes to the real server with the least number of connections)
Backup Server Group	If the health check feature detects failures in all the real servers in the server group, a server group can be specified to receive distribution as backup devices (standby devices).
Header Addition Feature※	Specifies whether to enable or disable the feature that adds the x-forwarded-for header to HTTP communication.

※ HTTP header packet more than 4096bytes can not be available.

INFO
- You can set the load-balancing method when you add server groups, and you can also change them after that.

Health Check Feature

The health check feature detects real server failures. It sends pings or ICMP pings to the TCP port of the real server at 2-second intervals. If they fail 4 times in a row it is judged that the relevant real server is experiencing communication interruptions.

If it is determined that the real server's communication is interrupted, the relevant real server is excluded from the load balancing destination server, and packets are no longer transferred. Instead, packets are sent to a different real server within the same server group.

After it has been determined that the real server's communication is interrupted, it sends pings or ICMP pings to the TCP port of the real server at 30-second intervals. If the ping succeeds twice in a row, it is determined that the communication has been recovered. The real server is automatically reset into the load balancing destination server, and packet transmission resumes.

INFO
- You can set the health check method from the Customer Portal.
- You can set health check methods for each server group.
- You can set the same health check method to multiple server groups.
- You can set TCP or ICMP as protocols for performing health checks. The operations are shown below.

Item	ICMP	TCP
Monitoring Content	Performs ICMP Ping monitoring	Specifies the ports to be

			monitored and performs TCP port monitoring.
	Health Check Intervals	2 seconds	
	Heath check intervals during downtime	30 seconds	
	Number of times before it is seen as down	4 times	
	Number of times before it is seen as recovered	2 times	
	Wait time between sending SYN and receiving ACK	-	1 second

5.8.3 Routing Feature

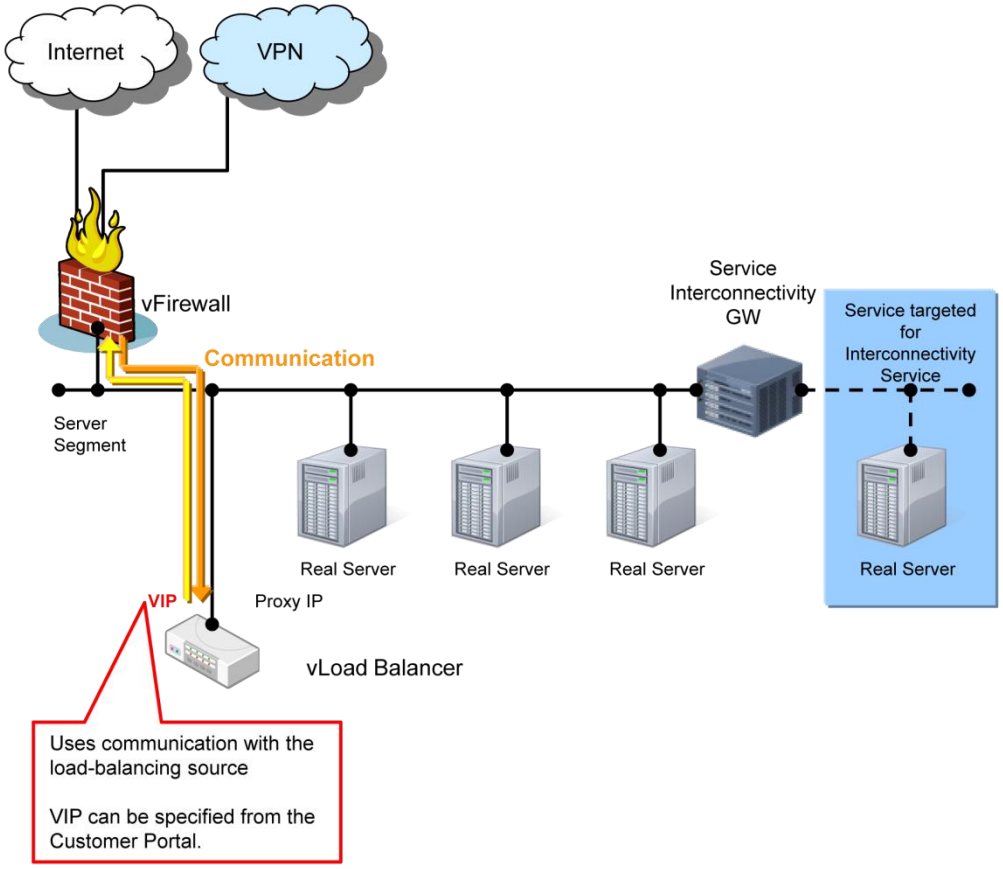
This is a feature that can set static routing to vLoad Balancer.

5.8.4 IP Address Delivery Feature

VIP

- VIP is a virtual IP address that is used when the load-balancing source and vLoad Balancer communicate. It is provided as an alias IP to the Server Segment side interface of vLoad Balancer.
- You can register multiple VIPs for one interface. You can set the maximum number of VIP using "VIP setting number" in vLoad Balancer resource.
- You can select VIPs from the available IP addresses in the Server Segment where the vLoad Balancer is installed. You can specify them from the Customer Portal when adding VIPs. VIPs are set as alias, active, or standby.

  Unspecified VIPs will be allocated automatically.



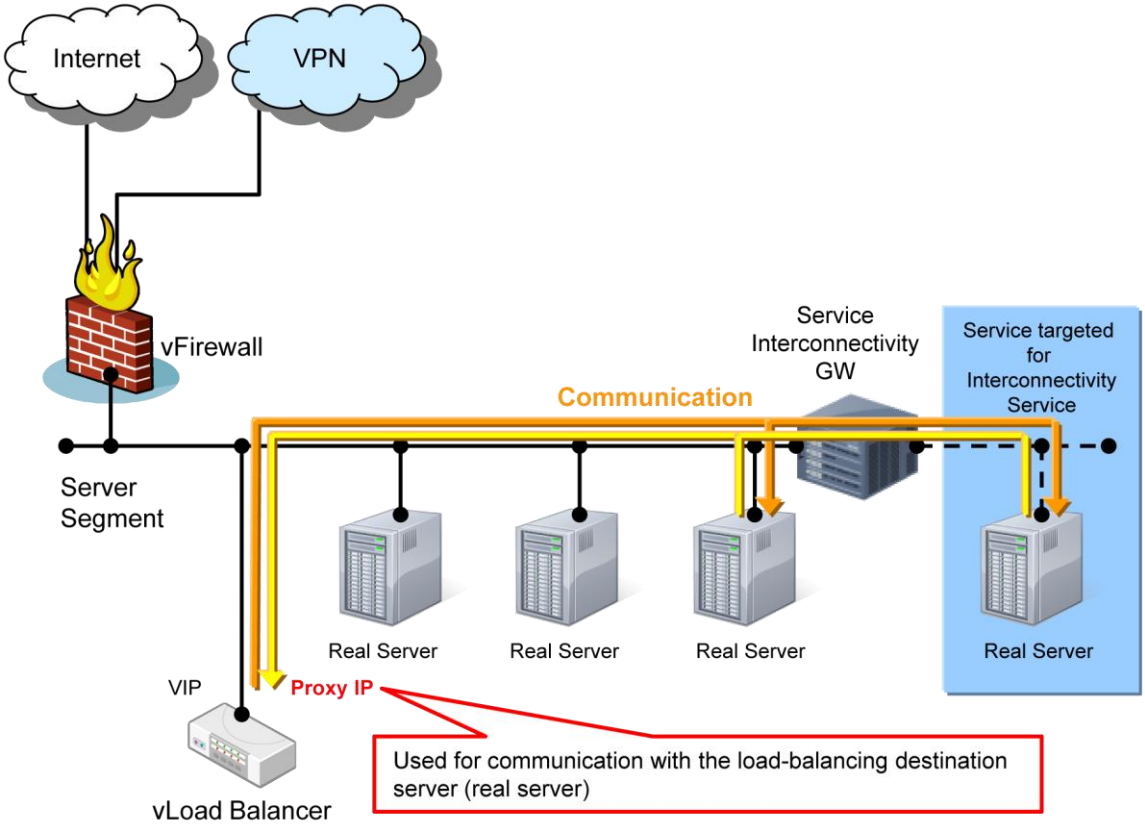
Proxy IP

- Proxy IP is a virtual IP address that is used when the real server and vLoad Balancer communicate. It is provided as an alias IP to the Server Segment side interface of vLoad Balancer.
- You can register multiple Proxy IPs for one interface.
- You can select Proxy IPs from the available IP addresses in the Server Segment where the vLoad Balancer is installed. You can specify them from the Customer Portal when adding Proxy IPs. Proxy IPs are set as alias, active, or standby.

  Unspecified Proxy IPs will be allocated automatically.
- The number of Proxy IPs used differs according to the vLoad Balancer resource value that is used. When you change the vLoad Balancer resource value, Proxy IP will automatically be added or reduced by the system.

vLoad Balancer Resource Value	Number of Proxy IP Used
1 to 2	1
3 to 4	2
5 to 6	3
7 to 8	4
9 to 10	5
11 or more	One for every two additional vLoad

	Balancer resource values



5.8.5 Important Points

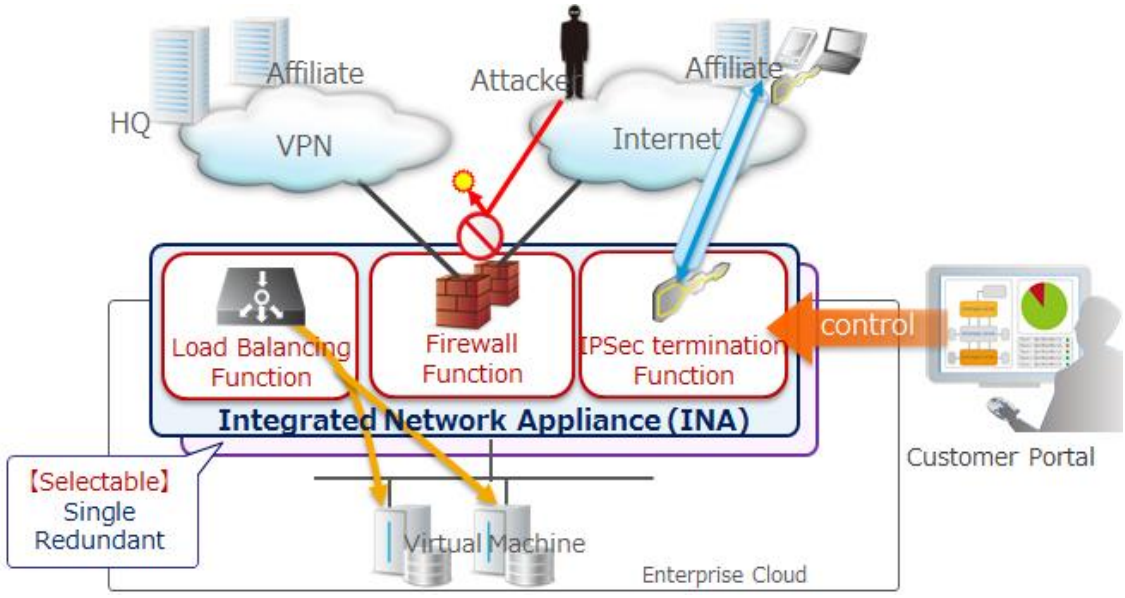
- In order to increase the vLoad Balancer resources, available IP addresses in the Server Segment are required.
- Communication interruptions might occur when you change vLoad Balancer settings from the Customer Portal.

5.9 Integrated Network Appliance

Integrated Network Appliance service is the service where the virtual network devices equipped with the firewall function, NAT/NAPT function, routing function, load balancing function and IPsec termination function are provided. With the Integrated Network Appliance service, one virtual network device dedicated for customers (called “Integrated Network Appliance” below is provided. Various parameters can be changed from Customer Port.

NOTE

- When starting to use the Integrated Network Appliance service, the stateful packet inspection function used for blocking illegal access by reading data of packets that pass through the Integrated Network Appliance and opening/closing ports according to its contents is enabled. This function cannot be disabled.



INFO

- Either the Integrated Network Appliance or vFirewall needs to be contracted for one Data Center in one Enterprise Cloud service contract. These services cannot be used simultaneously or multiple services cannot be used.

5.9.1 Available Features

Connection to each network

The Integrated Network Appliance can connect to the following networks.

Destination Network	Connection Conditions

Internet Transit	If the Internet Connectivity service is selected, connection to the Internet transit is always established.
VPN Transit	If the VPN Connectivity service is selected, connection to the VPN transit is always established.
Server Segment	If a Server Segment is added, connection to the Server Segment is provided. However, if “Do not connect to the Integrated Network Appliance.” is selected when adding a Server Segment, connection to the Server Segment is not provided.

Interfaces of the Integrated Network Appliance

Interfaces and allocatable IP addresses that are provided by the Integrated Network Appliance are shown below.

Interface	Allocatable IP Addresses
Virtual Network Interface for connecting to Internet Transit (called the "network interface on the Internet Transit-side" below)	NTT Communications selects IP addresses from the block for Global IP Addresses that are ordered separately
Virtual Network Interface for connecting to VPN Transit (called the "network interface on the VPN Transit-side" below)	NTT Communications selects IP addresses from the block for IP addresses of customer’s VPN (called the “IP address block for VPN Transit” below).
Virtual Network Interface for connecting to a Server Segment (called the "network interface on the Server Segment-side" below)	Customers can select the Virtual Network Interface from the available IP addresses in Server Segment (You can specify the IP address on the Server Segment-side network interface only when the Server Segment is created based on the application form. If IP addresses have not been specified, they will be allocated automatically).

NOTE

- IP addresses allocated to each interface of the Integrated Network Appliance cannot be changed after allocating them.

Main Features of the Integrated Network Appliance

Features and rules that can be set for the Integrated Network Appliance are shown below.

Features	Name of Available Rules	Details

Firewall feature	Firewall rule	This is the feature used for setting to allow/deny communications that pass through the Integrated Network Appliance.
NAT/NAPT feature	SNAT rule DNAT rule	This is the feature used for converting the IP address and ports for communications that pass through among Internet Transit, VPN Transit and Server Segment.
Routing feature	Static routing	This is the function used for providing the routing for communications that are made among Internet Transit, VPN Transit and Server Segment.
Load balancing feature	Load balancing rule	This is the function used for balancing load of communications from Internet Transit and VPN Transit.
IPsec termination feature	IPsec termination rule	This is the function used for terminating IPsec communications.

Plans of the Integrated Network Appliance

You can choose from the following four Integrated Network Appliance plans. Available performance and configurations vary depending on the plan that you order.

Plans	Performance	Configurations
Compact	For customers who do not use the load balancing feature and IPsec termination feature.	Single configuration
Compact (Redundant)	For customers who do not use the load balancing feature and IPsec termination feature.	Redundant configuration
Large	For customers who use the load balancing feature and IPsec termination feature.	Single configuration
Large (Redundant)	For customers who use the load balancing feature and IPsec termination feature.	Redundant configuration

NOTE

- The Integrated Network Appliance plan can be specified at the time of submitting the application form. After the network is opened, the plan cannot be changed from Compact to Large or vice versa. (It is possible

to change the plan from single configuration to redundant configuration or vice versa.)

INFO

- If the redundant configuration plan is selected, the hot standby configuration is provided and the plan is switched in approximately 30 seconds. Even if the single configuration plan is selected, the redundant configuration is adopted for basic equipment, equipment restart with the basic equipment for backup in case of failure and the configuration is switched approximately 5 to 10 minutes.
- All functions are available with Compact plan. However, Large plan is recommended when using the Load Balancing function and IP sec termination function due to the plunge in performance.

5.9.2 Firewall Feature

With this feature, the firewall rules for allowing or denying specific IP packets of communications that pass through the Integrated Network Appliance can be configured.

The following conditions can be specified for each firewall rule as the condition for IP packet to which the firewall rule is applied.

Item	Details
Firewall Rule	Customer can configure arbitrary rule names.
Source IP Address	Specifies a source IP address for IP packets.
Source Service	Specifies the source service for IP packets with the port number when setting TCP/UDP ports for protocol. If ICMP is specified for protocol, ICMP Type cannot be specified.
Destination IP Address	Specifies a destination IP address for IP packets.
Destination Service	Specifies the destination service for IP packets with the port number when setting TCP/UDP ports for protocol. If ICMP is specified for protocol, ICMP Type cannot be specified.
Protocol	Specifies the protocol used for IP packets (TCP, UDP or ICMP).
Actions	Specifies whether to allow or deny the passage of IP packets that match the conditions set by the above-mentioned items.
Enable	Enables/ disables this rule.

NOTE

- The firewall feature is set to deny all communications at the time of opening. Settings for enabling specific communications are required to allow communications.

INFO

- Priority of firewall rules can be set by changing the display order on the Customer Portal. Higher display order on the Customer Portal has higher priority level.

5.9.3 NAT/NAPT Feature

You can set IP Address Translation and IP Address Port Translation (called "SNAT/DNAT" below) rules for communications that pass through the Integrated Network Appliance.

There are 2 types of NAT/NAPT rules for the Integrated Network Appliance.

- ✧ NAT/NAPT for converting the source IP (called “SNAT” rule below)
- ✧ NAT/NAPT for converting the destination IP (called “DNAT” rule below)

SNAT Feature

The following items can be set for one SNAT rule.

Item	Details
Targeted network	Selects the destination network for communications to which the SNAT rule is applied from Internet Transit, VPN Transit and Server Segments that are connected to the Integrated Network Appliance.
Source IP address before conversion	Specifies the IP address that is not converted according to this rule.
Source IP address after conversion	Specifies the IP address that is converted according to this rule.
Enable	Enables or disables this rule.

DNAT Feature

The following items can be set for one DNAT rule.

Item	Details

Targeted network	Selects the destination network for communications to which the DNAT rule is applied from Internet Transit, VPN Transit and Server Segments that are connected to the Integrated Network Appliance.
Source IP address before conversion	Specifies the IP address that is not converted by this rule.
Destination port number before conversion/ ICMP Type	If TCP or UDP is specified for protocol, specify the port number that is not converted according to this rule. If ICMP is specified for protocol, ICMP Type needs to be specified.
Source IP address after conversion	Specifies the IP address that is converted according to this rule.
Destination port number after conversion/ ICMP Type	If TCP or UDP is specified for protocol, specify the port number that is not converted according to this rule. If ICMP is specified for protocol, ICMP Type needs to be specified.
Protocol	Specifies the protocol (TCP/ UDP/ ICMP) for communications to which this rule is applied.
Enable	Enables or disables this rule.

INFO

- You can translate IP addresses either 1 to 1 or 1 to N.
- The IP addresses that can be set to NAT/NAPT differ depending on the network that executes NAT/NAPT.

Network Type	Allocatable IP Addresses
Internet Transit	Global IP Address that is not allocated to Internet GW in global IP addresses that are used for Internet Connectivity
VPN Transit	Unused IP address from the IP address block that is allocated to VPN Transit
Server Segment	Any IP address in the IP address block allocated to the Server Segment

5.9.4 Routing Feature

The Integrated Network Appliance is equipped with the feature that establishes connection of Internet Transit, VPN Transit and Server Segment and executes the routing among them. In addition, the static routing can be set.

Static Routing

Static routing can be set to the Integrated Network Appliance.

Following are routing conditions that can be configured for each routing setting.

Item	Details
Static routing name	Customer can set arbitrary rule name.
Network	Specifies the destination L3 network for target communications.
Next hop	Specifies the next hop.
Targeted network	Selects the L2 network that is the next destination of communications to which this rule is applied from Internet Transit, VPN Transit and Server Segment that are connected to the Integrated Network Appliance.

INFO

- If Internet Connectivity and VPN Connectivity are used simultaneously, communications that directly relay back between Internet and VPN. If NTT Communications detect the settings that execute such communications, we may delete settings or restrict communications without advanced notice.
- The routing in which the same interface is used for the input interface and output interface cannot be set.

Default Route

Default route of the Integrated Network Appliance can be set. Following are items that can be set for the default route.

Item	Conditions
Internet Transit	When using the Internet Connectivity, Internet Transit can be selected for the default route.
VPN Transit	When using the VPN Connectivity, VPN Transit can be selected for the default route.

5.9.5 Load Balancing Feature

You can set load balancing rules that realize distribution of communication load by distributing communications that are terminated with the specific IP address allocated to the Integrated Network Appliance.

You can set the following items for each load balancing rule.

Item	Details
Load balancing rule name	Customer can set arbitrary rule name.
Explanation	Customer can arbitrarily input the explanation of this rule.
IP address	This is the IP address disclosed to client. This rule is applied to communications in which this IP address is set for the destination IP address.
Pool	Specified the destination server pool in this rule (server pool is described later).
Protocol	Specifies the protocol to which this rule is applied.
Session Maintenance Method	Selects the method for maintaining sessions according to this rule.
Enable	Enables or disables this rule.

Server Pool of Load Balancing

Multiple servers to which load are distributed according to the load balancing rules can be registered as server pool. You can set the following items for each server pool.

Item	Details
Server pool name	Customer can set arbitrary pool name.
Explanation	Customer can arbitrarily input the explanation of this server pool.
Member	Registers one server or multiple servers in this server pool.
Protocol	Specifies the protocol of communication to be distributed and transmitted to each server.
Port	Specifies the port number of communication to be distributed and transmitted to each server.
Protocol for monitoring	Selects the protocol for executing the health check for servers registered in the server pool.
Load balancing method	Selects the load balancing method when load is distributed to this server pool.

INFO

- IP addresses that can be specified for the load balancing rule differ depending on the network in which communication is established.

Network Type	Allocatable IP Addresses
Internet Transit	Global IP Address that is not allocated to Internet GW in global IP addresses that are used for Internet Connectivity.
VPN Transit	Unused IP address from the IP address block that is allocated to VPN Transit
Server Segment	Any IP address

- Health check is executed for each server that is registered as a member in the server pool with the following settings.

Item	Details	Value
Intervals	Health check intervals	5 seconds
Timeout	Threshold value for determining as timeout	15 seconds
Threshold value for healthiness	Number of times of success for determining as it is recovered	2 times
Threshold value for unhealthiness	Number of times of failure for determining as it is failed.	3 times

- The source IP of communication in which the load balancing rule is applied and delivered to each server in the server pool is the IP address allocated to the Server Segment-side interface in the Integrated Network Appliance. However, x-forwarded-for setting is enabled in default setting; therefore the source IP address in which SNAT is not applied can be checked by checking the http header.

5.9.6 IPsec Termination Function

It is possible to configure settings for terminating the IPsec communication in the Integrated Network Appliance. IPsec communication, which is the target of this function, is the IPsec communication that enables L3 communication between the Server Segment and the external VLAN by encrypting the Server Segment and the Server Segment in the customer's base or other Enterprise Cloud Service contract (called "external VLAN" below for these Server Segments).

You can set the following items for the IPsec termination rule.

Item	Details
IPsec termination rule name	Customer sets arbitrary rule name.
Explanation	Customer inputs the explanation of this IPsec termination rule.
Local Network	Specifies the Server Segment that is connected to external VLAN via IPsec communication.
Peer Network	Specifies the IP subnet of the external VLAN connected by using IPsec communications.
Local Endpoint	Specifies the interface of the Integrated Network Appliance that terminates IPsec communication.
Local ID	Specifies a unique ID that is configured at the Integrated Network Appliance in use arbitrarily in order to certify the target party's VPN device.
Peer ID	Inputs the ID specified by the IPsec termination equipment at the external VLAN side in order to certify the target party's VPN device.
Peer IP	Inputs the fixed IP used for IPsec communication that is allocated to the IPsec termination equipment at the external VLAN side.
Encryption Protocol	Specifies the encryption protocol (AES,AES256,3DES) that is used for IPsec communications (the common encryption protocol is used at Phase 1 and Phase 2).
Shared key	Specified the shared key used for authentication.
MTU	Sets the maximum value of one frame that is sent/ received through IPsec communications.
Enable	Selects whether to enable or disable this rule.

NOTE

- This is the feature that enables the setting for terminating IPsec communication. Actual connectivity is not included in this service.
- To establish IPsec communications, equipment for IPsec communication is required at the external VLAN side apart from this function. Customer needs to prepare equipment at the external VLAN side. Equipment at the external VLAN side is not supported by NTT Communications. (If the external VLAN is the Server Segment within the Enterprise Cloud service contract, the setting for establishing IPsec communications with mutual Integrated Network Appliance is available.)

INFO

- It is possible to configure the settings where one Server Segment and one external VLAN can be connected. When attempting to establish 1-to-N or N-to-1 connections, multiple IPsec termination rules need to be combined.
- It is possible to terminate IPsec communications that pass Internet Transit or VPN Transit. IPsec communication that passes through the Server Segment cannot be terminated.
- Do not perform multicast communications or broadcast communications through IPsec communications. If NTT Communications finds these communications, we may take actions, such as restriction on communications, without prior notice.
- Active mode is not supported by this feature; therefore Peer IP needs to be the fixed IP that can be connectable from the Integrated Network Appliance.
- The following items are configured as default settings of the Integrated Network Appliance.

Parameter		Value
Key management protocol		IKEv1(ISAKMP + Oakley)
Phase1	Authentication Method	pre-shared key
	DH group	2
	Hash Algorithm	SHA1
	ISAKMP SA life time	28800 seconds
	key exchange mode	Main mode
Phase2	IPsec SA life time	3600 seconds
	Security protocol	ESP
	Authentication Algorithm	HMAC-SHA1
	Perfect Forward Secrecy	Enable
	DH group	2
	Capsuling mode	Tunnel
	key exchange mode	Quick mode

5.9.7 Important Points

Rules Set by NTT Communications (Global Rule)

Multiple rules (called “Global Rule” below) are configured for the Integrated Network Appliance in default setting to allow NTT Communications to perform monitoring, maintenance and operation and provide various services.

- Customer can refer the Global Rule. However, please note that we may not be able to answer questions regarding specific purpose and details of the Global Rule.
- Customer cannot edit or delete the Global Rule.
- The Global Rule is set as the rule having the higher priority than various rules set by customer.
- Please note that the Global Rule may be added, changed or deleted by us without prior notice.

NOTE

- When monitoring the virtual server starts, SNAT rule and DNAT rule are added to the virtual server to be monitored for each virtual server to be monitored.

Number of Configurable Rules

For the Integrated Network Appliance, the following number of rules can be set regardless of the plan.

Feature	Maximum number of rules that can be set
Firewall rule	Approximately 90 rules
SNAT rule DNAT rule	Approximately 190 rules (including SNAT rule and DNAT rule)
Static routing	Approximately 90 rules
Load balancing rule	Approximately 3 rules
IPsec termination rules	Approximately 50 rules

INFO

- The above maximum number of rules that can be set includes the number of Global Rules. The value obtained by subtracting the number of Global Rules from the above values is the number of rules that can be set by customer.
- Performance is likely to be degraded when the number of rules set increases.

Restrictions and Disclaimers

- Although it is possible to set various communication rules by using this service, customers are responsible for setting contents; therefore NTT Communications cannot guarantee validity and accuracy of setting contents. In addition, we cannot compensate damages caused by defects of the setting contents (However, we are responsible for setting the Global Rules).
- Communication interruptions might occur when you change the settings of the Integrated Network Appliance from the Customer Portal.
- Performance monitor is not available in Customer Portal.
- The case where IP address below and routing settings are the same NTT Communications does not support the operation.
  - Global IP address
  - VPN transit IP address block
  - Server Segment IP address block
  - Non-duplicatable IP Address Bands indicated to Important Point in Server Segmet section

5.9.8 Reference Information

Various Recommended Values of the Integrated Network Appliance

Various recommended values are as follows.

Item	Recommended Value	Details
Performance	Approximately up to 100Mbps	Although performance is not restricted, approximately up to 100Mbps is expected regardless of plans based on results of verification. In addition, performance is degraded in inverse proportion to increase of the number of rules set.
Number of load balancing rules	3	Although it may be possible to set 3 or more rules depending on customer's usage situation, we can only support up to 3 rules.
Number of virtual servers in use	Approximately 20	Two NAT rules are set for one VM as Global Rules in order to execute VM monitoring. Along with these rules, a maximum of 4 NAT rules are consumed if NAT rules are set for communications for Internet; therefore using approximately 20 VMs is expected.
Downtime in case of redundancy plan	Approximately 30 seconds	When using the redundant plan, recovery with downtime of approximately 30 seconds is expected.

Recommended Environment for IPsec Termination Function

The checking-of-operations model by our company is as follows.

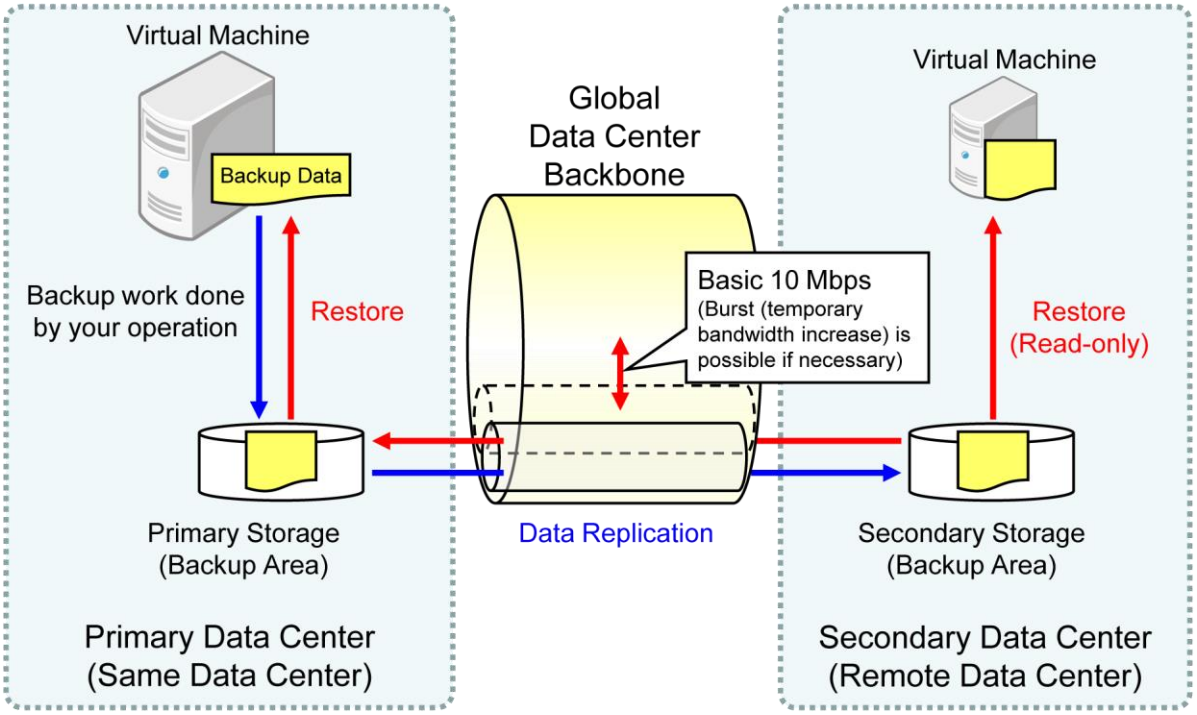
- ASA5510
- Vyatta Core 6.6R1
- Integrated Network Appliance (this service)

※ NTT Communications does not support about actual connectivity.

6. External Storage (Global Standard Menu)

6.1 Global File Storage (Global Data Backup)

Global File Storage (Global Data Backup) is a service that provides shared External Storage areas for storing backup data. It provides a feature that stores backup data not only in the Primary Data Center (the same Data Center) but also stores backup data in a Secondary Data Center (remote Data Center).



INFO

- The shared External Storage area is connected by CIFS (Common Internet File System) protocol or NFS (Network File System) protocol.
- We ask you to run the backup data storage operation.
- Global File Storage (Global Data Backup) is used via Service Interconnectivity. You need to apply separately for Service Interconnectivity.

6.1.1 Available Features

You can use the following features with Global File Storage (Global Data Backup).

Feature	Overview
Provides storage for saving data	A feature that uses the shared External Storage area for storing backup data. You can choose from the following two plans. ● Local DC Storage (provides Primary Storage only) ● Remote DC Storage (provides Primary and Secondary storages)
Data replication feature (burst feature)	If you have selected the Remote DC Storage Plan, this feature transfers the data to Remote DC Storage.

INFO

- The connection to the shared External Storage area uses CIFS protocol or NFS protocol.
- You can retrieve data that is in Primary or Secondary storage.
- It is possible to temporarily increase the transmission speed of the virtual network with bursts, according to the traffic volume. The transmission speed for bursts differs according to the service plan (S/M/L).

6.1.2 Provides Storage for Saving Data

You can install and set up primary storage that can be connected by CIFS protocol or NFS protocol over a previously-specified IP network, and use the shared External Storage area for storing backup data.

INFO

- The backup storage specified by NTT Communications is used in the shared External Storage area of Global File Storage (Global Data Backup). The head unit of the storage used for backup is in a cluster structure and the parity Disks are redundant.
- The connection with Primary Storage is through Service Interconnectivity. The transmission speed provided is Best Effort. It varies depending on your system environment and the status of line congestion.
- A maximum of 10 Storage units can be used with a single Service Interconnectivity.

Plans

You can choose from the following Storage plans.

Plans	Overview
Local DC Storage	As backup area, the plan provides only the shared External Storage area (Primary Storage) inside the same Data Center (Primary Data Center).
Remote DC Storage	In addition to the Local DC Storage Plan, the plan provides a data replication feature. You can transfer data from Primary Storage to a shared External Storage area (Secondary Storage) installed in a remote Data Center (Secondary Data Center).

INFO

- If you are separately using a Compute Resource at a remote Data Center, you can retrieve data stored in Secondary Storage from the remote Data Center via Service Interconnectivity. To use this service, you must submit an application in writing.
- When you connect from the Compute Resource at the remote Data Center, Secondary Storage is read-only. You cannot store newly-created data.
- You can save to the remote Data Center by connecting between Data Centers using a virtual network.
- It is possible to temporarily increase the transmission speed of the virtual network with bursts, according to the traffic volume. The transmission speed for bursts differs according to the service plan (S/M/L).

Storage Capacity

You can increase or decrease the storage capacity of a single shared External Storage area within the range listed below.

	Lower Limit	Upper Limit	Setting Unit
Storage Capacity	500 GB	4,000 GB	100 GB

※ 1 GB is 1,024 bytes to the power of 3.

NOTE

- If you reduce storage capacity, you cannot specify a capacity smaller than the volume of the stored data.

Protocol Used

You can choose CIF or NFS as the protocol for connecting to the shared External Storage area (Primary Storage).

Note that the method for limiting the users who can use the primary storage differs according to protocol.

Protocol Used	Protocol Version	Remarks
NFS	NFS version 3	The users who can use Primary Storage are limited according to the IP address and Server Segment of the connection source.
CIFS	SMB 1.0 or SMB 2.0	The users who can use Primary Storage are limited according to WORKGROUP user and password.

INFO
- If you use CIFS protocol, please set the WORKGROUP user and password permitting use of Primary Storage according to the rules specified by NTT Communications.
- If you use CIFS protocol, the shared name will be set automatically.
- You cannot use both NFS protocol and CIFS protocol for a single Primary Storage.

6.1.3 Data Replication Feature (Burst Feature)

To manage the remote DC, you can use a data replication feature that synchronizes data between Primary Storage and Secondary Storage.

INFO
- The data that is transferred using data replication is differential data after the time of the previous data synchronization.

Virtual Network Used for Replication

A virtual network is provided to use for replication between Primary Storage and Secondary Storage.

It is possible to temporarily increase the transmission speed of the virtual network with bursts, according to the traffic volume. The transmission speed for bursts differs according to the service plan (S/M/L).

Plans	Basic Transmission Speed	Transmission Speed During a Burst
S Plan	10 Mbps	50 Mbps
M Plan	10 Mbps	100 Mbps
L Plan	10 Mbps	500 Mbps

Note that the basic transmission speed and the transmission speed during a burst are both provided on a Best Effort basis.

NOTE

- The virtual network for replication is a Best Effort type service that changes the transmission speed according to your system environment and line congestion. The actual transmission speed varies according to the usage of other customers and infrastructure status. The service does not guarantee transmission speed.

INFO

- During the period of time that burst is running, a burst charge applies. It is charged by the minute.
- If data replication finishes while burst is running, it will be automatically detected within the prescribed amount of time and burst will terminate automatically.

Timing of Data Replication

You can choose from any of the following types of timing for replication from Primary Storage to Secondary Storage and for burst timing.

Replication Method	Timing
Repetition schedule	A replication schedule is registered, and replication is run periodically according to the schedule.
Reserved schedule	A date (any 1 date) and time are scheduled, and replication is run according to the schedule.
Manual immediate execution	The replication is run by manual operation.

NOTE

- It is not possible to replicate data automatically every time data is changed.

Restore

Even if the data was replicated from Primary Storage to Secondary Storage, data is restored manually from the following directories and folders, which were created in Primary Storage. Note that the directory and folder names will differ according to the protocol used.

Protocol Used	Directory/Folder
NFS	.snapshot
CIFS	~snapshot

INFO

- The data that was last replicated (the same data as that saved in Secondary Storage) is stored in the above-mentioned directories and folders.
- Restore from Secondary Storage to Primary Storage is limited to situations where the primary Data Center can no longer be used, such as during disasters, and is executed at the judgment of NTT Communications.

6.1.4 Important Points

IP Address

It is necessary to allocate an IP Address Block with a Prefix Length of /29 to be used for Global File Storage (Global Data Backup). The number of IP addresses differs according to the contracted plan.

Plans	Number of IP Address Blocks	IP Addresses Allocated from the IP Address Block
Local DC Storage	1	• Primary storage IP address • Service Interconnect Gateway IP address
Remote DC Storage(data storage only)	2	• Primary storage IP address • Service Interconnect Gateway IP address • Secondary Storage IP address
Remote DC storage (when using stored data at a remote DC)	3	• Primary storage IP address • IP address of the same Data Center's Service Interconnect Gateway • IP address of the remote Data Center's Service Interconnect Gateway • Secondary Storage IP address

NOTE

- You cannot change the address block or IP addresses used for the connection.

Restrictions

- Not just Customer-created data is saved in the shared External Storage area of Primary Storage. Metafiles used for administration are also saved.

  The data size of these administration metafiles is also included in the available capacity of Primary Storage, and this size increases according to the size of your data and other factors.
- You cannot link to a directory service.
- The paths for the Primary Storage name and mount are set automatically.

- If you delete the existing volume, the administered data is also deleted, and you will be unable to restore it.
- The default gateway IP address for Primary Storage is the IP address for the Service Interconnect Gateway.
- You cannot replace Service Interconnectivity once it has been set.
- You cannot set the storage capacity and connection protocol separately for Primary Storage and Secondary Storage. They are automatically set to be the same.
- You can specify only one Secondary Storage for one Primary Storage. You cannot specify multiple secondary storages.

7.Security Features (Global Standard Menu)

7.1 IPS/IDS

IPS/IDS is a service that detects and blocks unauthorized access and attack traffic.

INFO
- IPS/IDS is used via Service Interconnectivity. You need to apply separately for Service Interconnectivity.

7.1.1 Available Features

The following features are available for IPS/IDS.

Feature	Overview
IPS/IDS	A feature that detects and blocks unauthorized access and cyber-attacksc on the Virtual Machine.

7.1.2 IPS/IDS Feature

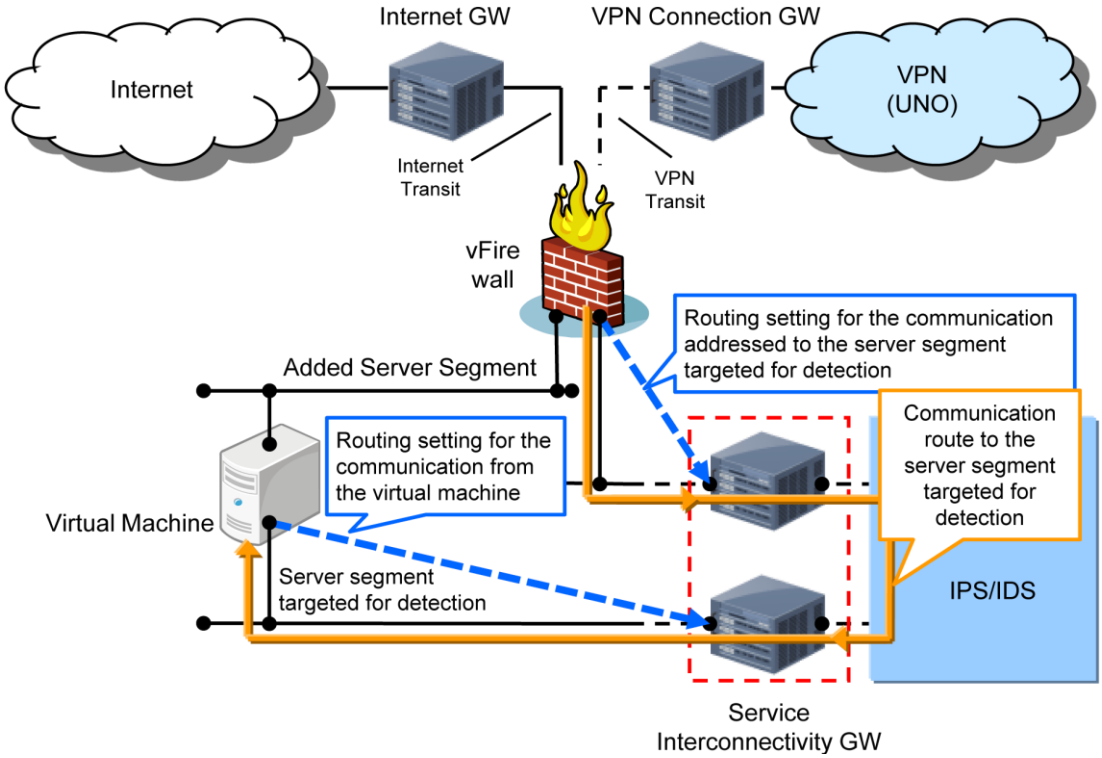
You can choose either IPS mode or IDS mode.

Mode	Overview
IPS	Unauthorized access and cyber-attacks are detected. When unauthorized access and cyber-attacks are detected, traffic is blocked.
IDS	Unauthorized access and cyber-attacks are detected. However, traffic is not blocked even though unauthorized access and cyber-attacks are detected.

INFO
- If NTT Communications judges it necessary, we will notify you via email, etc. of detection and blocking status (for IPS mode only).

Routing Settings

Only communication via IPS/IDS is targeted for detection. When you use IPS/IDS, please set the following routing.



- The communication addressed to Server Segments targeted for detection is set so that it is routed by vFirewall to the Service Interconnect Gateway used for IPS/IDS.
- The communication from the Virtual Machine is set so that it is routed by the Virtual Machine on the Server Segment targeted for detection to the Service Interconnect Gateway used for IPS/IDS.
- If you perform Ping monitoring on the Virtual Machine, you will require an additional Server Segment for direct connection between vFirewall and the Virtual Machine.

INFO
- Please do not connect the Server Segments targeted for detection directly to vFirewall.

Analysis Capacity

The traffic volume that can be analyzed by IPS/IDS is shown below.

Item	Performance		Remarks
	Per service	Maximum (5 services used)	
Traffic Processing Capacity	200 Mbps	1 Gbps	The total value of uplink and downlink.
Number of concurrent sessions	40,000	200,000	The number of sessions that can be connected simultaneously.

INFO
- You can increase the traffic volume up to 1 Gbps, 200,000 sessions (when 5 services are used) by applying additional services.

IPS Mode Simulation (Japan local feature)

Simulation is a process for improving the accuracy of IPS mode for detecting and blocking unauthorized access and cyber-attacks. You can choose whether to implement a simulation at the time of application for IPS/IDS. We recommend implementing it in order to reduce the amount of false positive detections.

If simulation is implemented, a simulation time period is set (approximately 1 – 4 weeks after you start using IPS mode) during which only detection of unauthorized access and attack traffic is performed and traffic is not blocked. After the simulation time period, please check to see whether the traffic that IPS/IDS detects as being targeted for blocking is normal traffic. Based on the results of the check, the IPS/IDS settings will be adjusted.

7.1.3 Important Points

Used IP Addresses

- In order to connect the Service Interconnect Gateway with IPS/IDS, you must have two IP address blocks available. If the IP address block is already being used, we might ask you to change it.
- NTT Communications will manage the assigned IP address blocks, and assign IP addresses to the devices that require them.

Restrictions

- When the actual traffic volume exceeds the contracted traffic volume, the excess traffic might be discarded.
- Encrypted communication is not targeted for detection or blocking.
- Packets which break TCP/UDP/IP protocol rules or abnormal packets are discarded as a standard function regardless of customer's configuration.

  (Examples)

  - When the IP header is cut off in the middle
  - When the Port number is 0 (zero)
  - When the TCP flag combination is abnormal and others
- If devices making up this feature are replaced due to malfunction etc., you will not be able to check device logs or event reports from prior to the replacement via the Security Web Portal. In addition, if the regular server and the standby server are switched for a redundantly configured device and they are restored without replacing the device, you cannot check the log or the event reports for the period during which the switching occurred from the Security Web Portal.
- IPS/IDS does not guarantee that the IPS/IDS feature has integrity or accuracy, or is suitable for your use. Furthermore, the suitability of the unauthorized/attack traffic

detection algorithms provided by the developers or distributors of the devices making up the IPS/IDS feature is not guaranteed.

- The following information might be provided to the developers or distributors of the devices making up the IPS/IDS feature.
  - Configuration information obtained from providing IPS/IDS
  - Information concerning controls etc. for IPS/IDS
- We cannot guarantee recovery from failures that might occur due to incompatibility between IPS/IDS and your environment, or failures that occur due to your operations other than those specified by NTT Communications.

7.2 Email-Anti-Virus

Email-Anti-Virus is a service that detects and blocks viruses that invade via Email (STMP communication).

INFO
- Email-Anti-Virus is used via Service Interconnectivity. You need to apply separately for Service Interconnectivity.

7.2.1 Available Features

You can use the following features in Email-Anti-Virus.

Feature	Overview
Virus scan	A feature that monitors email (STMP communication), and executes specified processes when viruses are detected.

7.2.2 Virus Scan Feature

SMTP is the protocol that is targeted for inspection by Email-Anti-Virus.

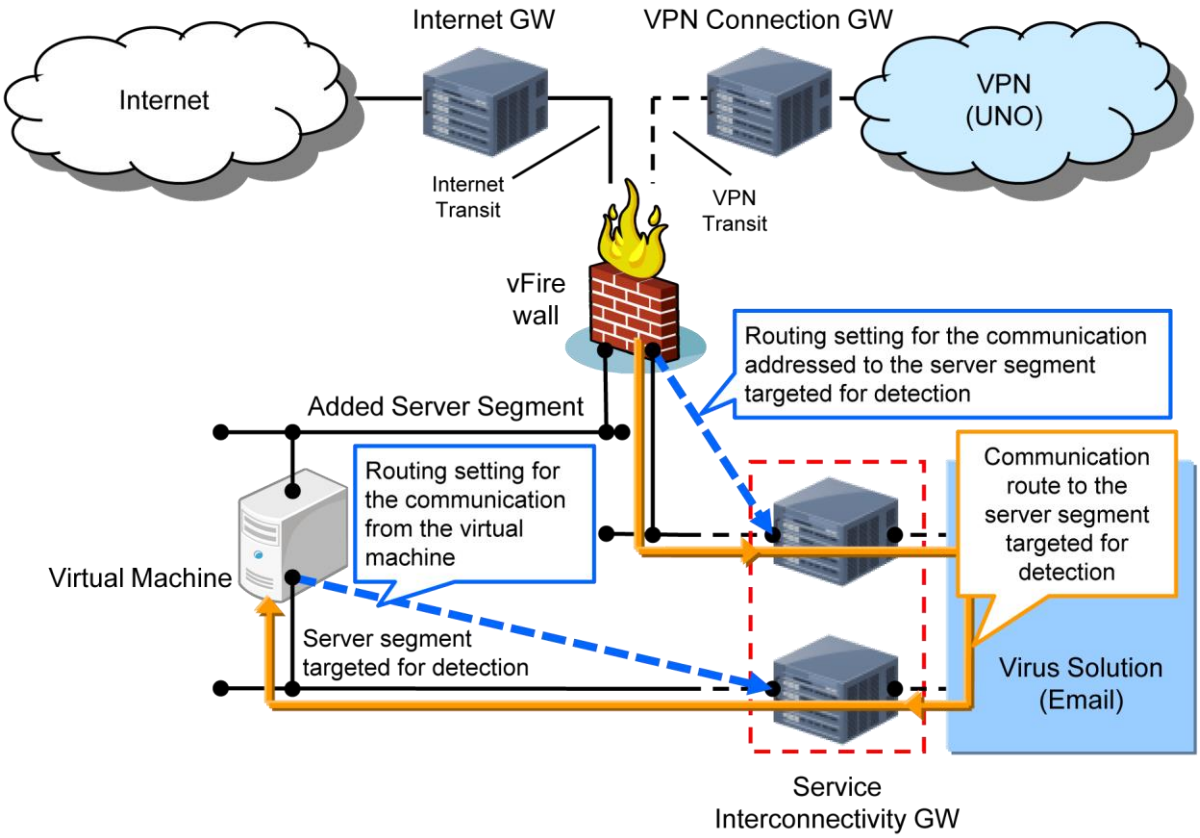
You can choose the detection and blocking operations. The detection and blocking processes are shown below.

Item	Process	Information Recorded in Logs
Allow	Allows communication.	None
Alert	Monitors email (SMTP), and detects viruses. However, traffic is not blocked even though viruses are detected.	Detection Status
Block	Monitors email (SMTP), and detects viruses. Note that communication is blocked when viruses are detected, and the SMTP Reply Code: 541 is returned to the sender.	Blocking status

INFO
- If NTT Communications judges it necessary, we will notify you via email, etc. of the detection and blocking status (for blocking only).

Routing Settings

Only communication via Email-Anti-Virus is targeted for detection. When you use Email-Anti-Virus, please set the following routing.



- The communication addressed to Server Segments targeted for detection is set so that it is routed by vFirewall to the Service Interconnect Gateway used for Email-Anti-Virus.
- The communication from the Virtual Machine is set so that it is routed by the Virtual Machine on the Server Segment targeted for detection to the Service Interconnect Gateway used for Email-Anti-Virus.
- If you perform Ping monitoring on the Virtual Machine, you will require an additional Server Segment for direct connection between vFirewall and the Virtual Machine.

INFO
- Please do not connect the Server Segments targeted for detection directly to vFirewall.

Analysis Capacity

The traffic volume that can be analyzed by Email-Anti-Virus is shown below.

Item	Performance		Remarks
	Per service	Maximum (5 services used)	
Traffic Processing Capacity	200 Mbps	1 Gbps	The total value of uplink and downlink.
Number of concurrent sessions	40,000	200,000	The number of sessions that can be connected simultaneously.

INFO
- You can increase the traffic volume up to 1 Gbps, 200,000 sessions (when 5 services used) by applying additional services..

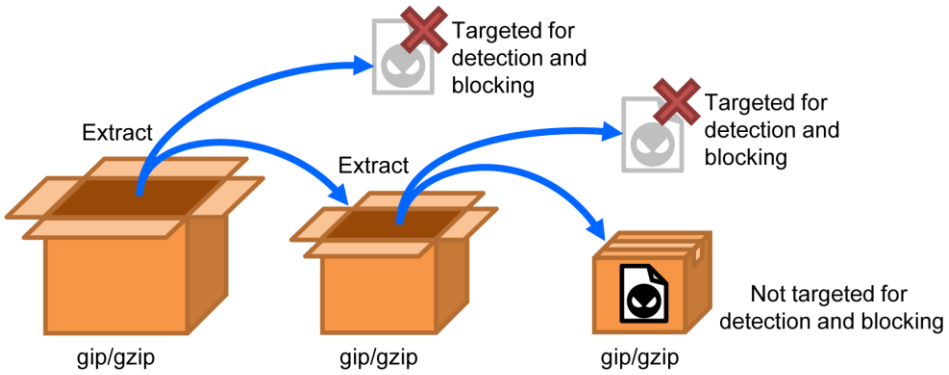
7.2.3 Important Points

Used IP Addresses

- In order to connect the Service Interconnect Gateway with Email-Anti-Virus, you must have two IP address blocks available. If the IP address block is already being used, we might ask you to change it.
- NTT Communications will manage the assigned IP address blocks, and assign IP addresses to the devices that require them.

Restrictions

- When the actual traffic volume exceeds the contracted traffic volume, the excess traffic might be discarded.
- The following files are not targeted for detection and blocking.
  - Encrypted files
  - Files set with passwords
  - Files compressed by compression algorithms other than zip/gzip format
  - Files compressed by compression algorithm zip/gzip format three times or more



Files that have been compressed using the zip/gzip compression algorithm are automatically extracted and are targeted for detection and blocking.

- Packets which break TCP/UDP/IP protocol rules or abnormal packets are discarded as a standard function regardless of customer's configuration.

  (Examples)

  - When the IP header is cut off in the middle
  - When the Port number is 0 (zero)
  - When the TCP flag combination is abnormal and others

- If devices making up this feature are replaced due to malfunction etc., you will not be able to check device logs or event reports from prior to the replacement via the Security Web Portal. In addition, if the regular server and the standby server are switched for a redundantly configured device and they are restored without replacing the device, you cannot check the log or the event reports for the period during which the switching occurred from the Security Web Portal.
- Email-Anti-Virus does not guarantee that the Email-Anti-Virus feature has integrity or accuracy, or is suitable for your use. Furthermore, the suitability of the virus identification algorithms provided by the developers or distributors of the devices making up the Email-Anti-Virus feature is not guaranteed.
- The following information might be provided to the developers or distributors of the devices making up the Email-Anti-Virus feature.
  - Configuration information obtained from providing Email-Anti-Virus
  - Information concerning inspections etc., for Email-Anti-Virus
- We cannot guarantee recovery from failures that might occur due to incompatibility between Email-Anti-Virus and your environment, or failures that occur due to your operations other than those specified by NTT Communications.

7.3 Web-Anti-Virus

Web-Anti-Virus is a service that detects and blocks viruses that invade via Web access (HTTP communication) and FTP communication.

INFO
- Web-Anti-Virus is used via Service Interconnectivity. You need to apply separately for Service Interconnectivity.

7.3.1 Available Features

You can use the following features in Web-Anti-Virus.

Feature	Overview
Virus scan	A feature that monitors Web access (HTTP communication) and FTP communication, and executes specified processes when viruses are detected.

7.3.2 Virus Scan Feature

HTTP and FTP are the protocols targeted for inspection by Web-Anti-Virus.

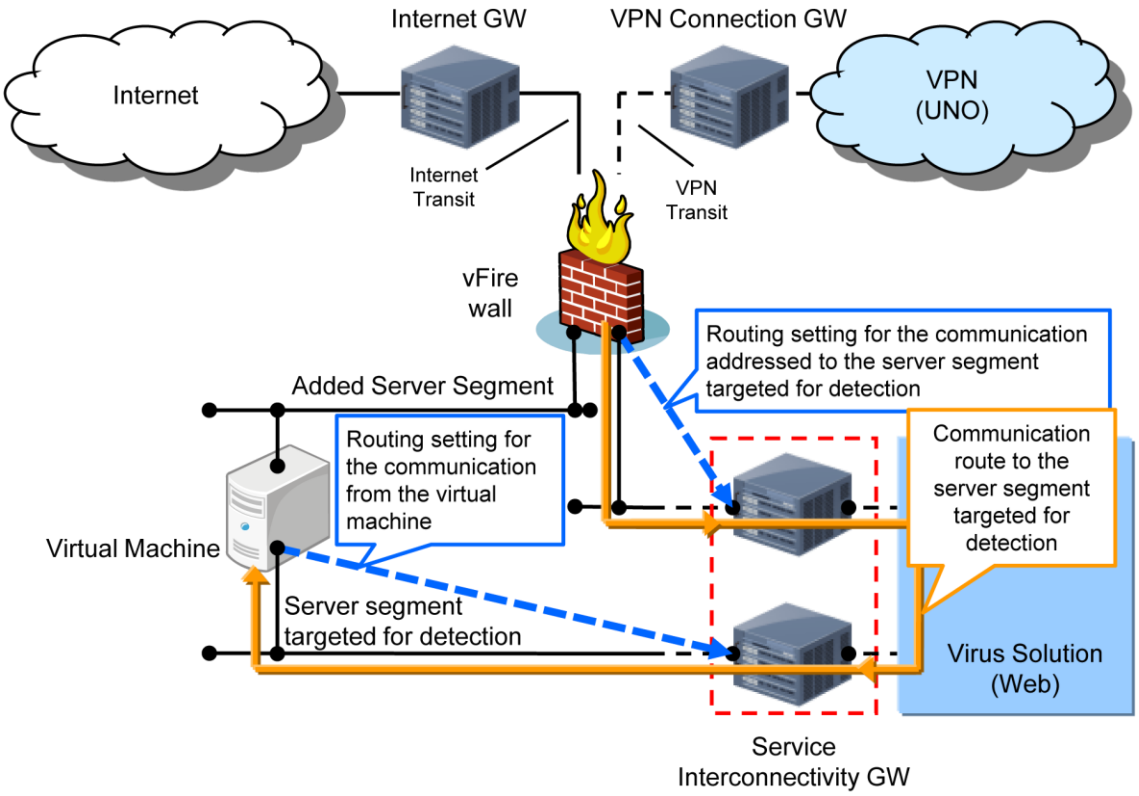
You can choose the detection and blocking operations for each protocol. The detection and blocking processes are shown below.

Item	Process	Information Recorded in Logs
Allow	Allows communication.	None
Alert	Monitors Web access (HTTP communication) and FTP communication, and detects viruses. However, traffic is not blocked even though viruses are detected.	Detection Status
Block	Monitors Web access (HTTP communication) and FTP communication, and detects viruses. Note that communication is blocked when viruses are detected, and a blocked screen is displayed to the user.	Blocking status

INFO
- If NTT Communications judges it necessary, we will notify you via email, etc. of the detection and blocking status (for blocking only).

Routing Settings

Only communication via Web-Anti-Virus is targeted for detection. When you use Web-Anti-Virus, please set the following routing.



- The communication addressed to Server Segments targeted for protection is set so that it is routed by vFirewall to the Service Interconnect Gateway used for Web-Anti-Virus.
- The communication from the Virtual Machine is set so that it is routed by the Virtual Machine on the Server Segment targeted for protection to the Service Interconnect Gateway used for Web-Anti-Virus.
- If you perform Ping monitoring on the Virtual Machine, you will require an additional Server Segment for direct connection between vFirewall and the Virtual Machine.

INFO
- Please do not connect the Server Segments targeted for detection directly to vFirewall.

Analysis Capacity

The traffic volume that can be analyzed by Web-Anti-Virus is shown below.

Item	Performance		Remarks
	Per service	Maximum (5 services used)	
Traffic Processing Capacity	200 Mbps	1 Gbps	The total value of uplink and downlink.

Number of concurrent sessions	40,000	200,000	The number of sessions that can be connected simultaneously.

INFO
- You can increase the traffic volume up to 1 Gbps, 200,000 sessions (when 5 services used) by applying additional services.

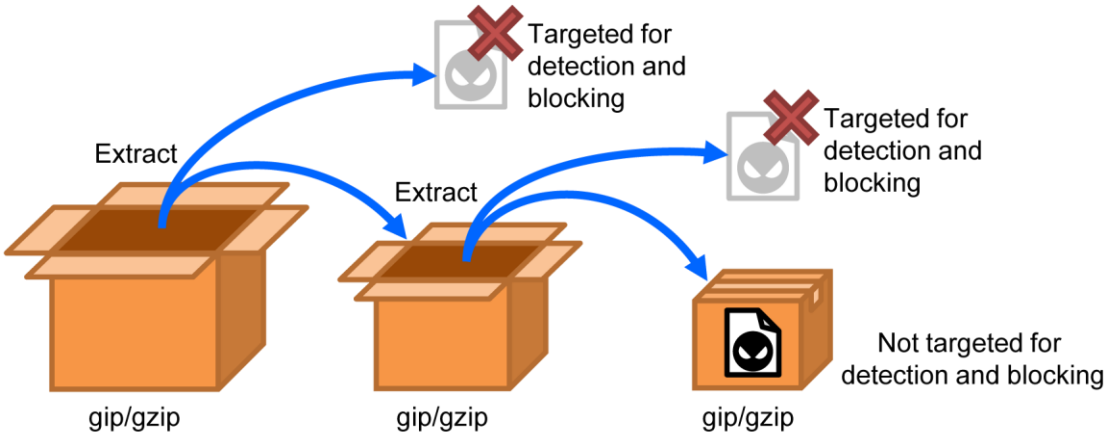
7.3.3 Important Points

Used IP Addresses

- In order to connect the Service Interconnect Gateway with Web-Anti-Virus, you must have two IP address blocks available. If the IP address block is already being used, we might ask you to change it.
- NTT Communications will manage the assigned IP address blocks, and assign IP addresses to the devices that require them.

Restrictions

- When the actual traffic volume exceeds the contracted traffic volume, the excess traffic might be discarded.
- The following communication and files are not targeted for detection and blocking.
  - Encrypted communication (that used HTTPS or SFTP, etc.)
  - Files set with passwords
  - Files compressed by compression algorithms other than zip/gzip
  - Files compressed by compression algorithm zip/gzip three times or more



Files that have been compressed using the zip/gzip compression algorithm are automatically extracted and are targeted for detection and blocking.

- Packets which break TCP/UDP/IP protocol rules or abnormal packets are discarded as a standard function regardless of customer's configuration.

  (Examples)

  - When the IP header is cut off in the middle

  - When the Port number is 0 (zero)
  - When the TCP flag combination is abnormal and others
- If devices making up this feature are replaced due to malfunction etc., you will not be able to check device logs or event reports from prior to the replacement via the Security Web Portal. In addition, if the regular server and the standby server are switched for a redundantly configured device and they are restored without replacing the device, you cannot check the log or the event reports for the period during which the switching occurred from the Security Web Portal.
- Web-Anti-Virus does not guarantee that the Web-Anti-Virus feature has integrity or accuracy, or is suitable for your use. Furthermore, the suitability of the virus identification algorithms provided by the developers or distributors of the devices making up the Web-Anti-Virus feature is not guaranteed.
- The following information might be provided to the developers or distributors of the devices making up the Web-Anti-Virus feature.
  - Configuration information obtained from providing Web-Anti-Virus
  - Information concerning detection etc., for Web-Anti-Virus
- We cannot guarantee recovery from failures that might occur due to incompatibility between Web-Anti-Virus and your environment, or failures that occur due to your operations other than those specified by NTT Communications.

7.4 URL Filtering

URL Filtering is a service that controls access to websites in accordance with the policies of the customer.

INFO

- URL filtering is used via Service Interconnectivity. You need to apply separately for Service Interconnectivity.
- URL Filtering filters communication from the client (VPN) to the Server Segments targeted for protection.

7.4.1 Available Features

You can use the following features in URL Filtering.

Feature	Overview
URL filtering	A feature that controls website access by either issuing a warning or blocking websites according to website categories supplied by URL filtering.

7.4.2 URL Filtering Feature

The protocols targeted for URL filtering detection are HTTP and HTTPS.

INFO

- URL filtering for HTTPS is implemented using domains.
- HTTPS communication is determined based on the URL in the Common Name of the server certificate.

Configuring Category Operations

With URL filtering, websites targeted for control are divided in advance into categories and registered, and you can choose warning and blocking operations for each category. The content of the warning and blocking processes are shown below.

Item	Process	Information Recorded in Logs
Allow	Allows communication.	None
Alert	Allows communication.	URL of access-restricted website
Continue	If users access websites that are registered in those categories, a warning screen indicating that they have accessed a restricted website is displayed. If users click the "Continue" button on the displayed warning screen, they can access the website in question.	URL of access-restricted website

Block	If users access websites that are registered in those categories, a screen indicating that they have accessed a restricted website is displayed and the website is blocked. The user cannot access the relevant website.	URL of access-restricted website

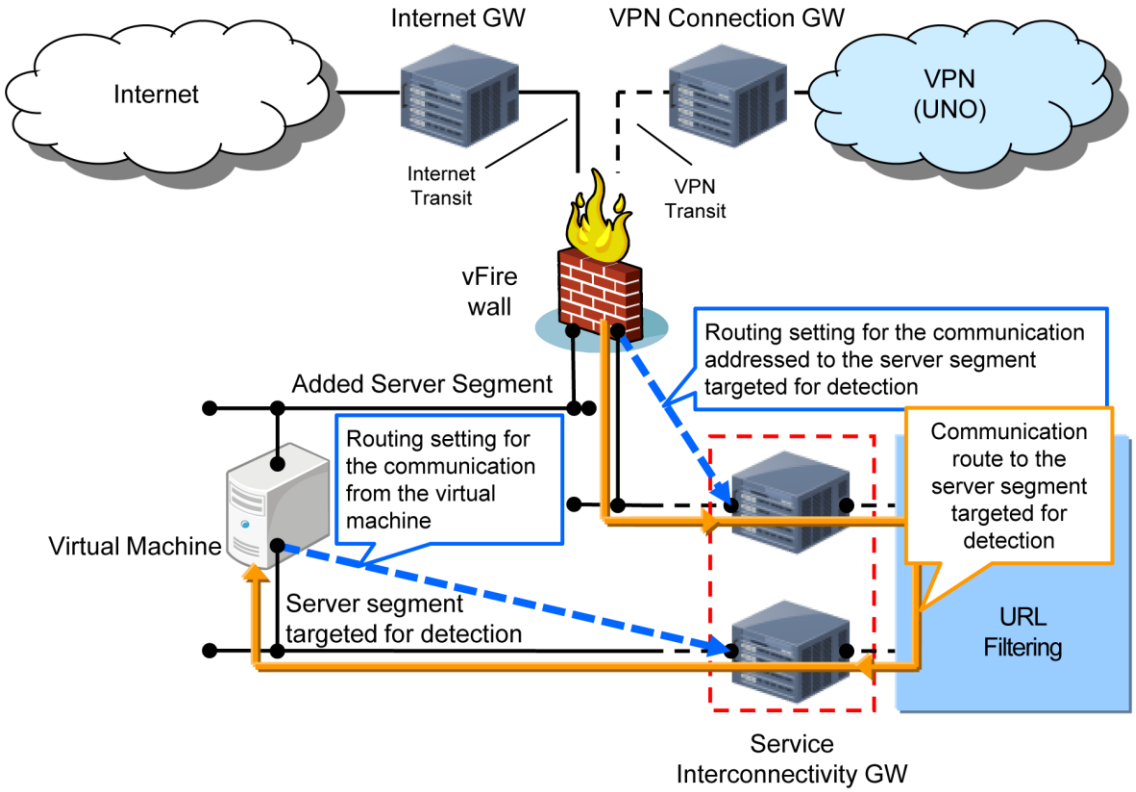
Configuring Controlled Websites

As needed, you can add or delete the websites targeted for control that are registered in each category.

Feature	Overview
Allowed URL (White list)	From the group of websites that are registered to categories that are set as "warning" or "blocking", you can specify a URL as an exception and allow access. A maximum of 100 URLs can be registered.
Prohibited URL (Blacklist)	From the group of websites that are registered to categories that are set as "permission", you can specify a URL as an exception and prohibit access (block). You can register a URL that is not registered in any category and prohibit access (block). A maximum of 100 URLs can be registered.

Routing Settings

Only communication via URL Filtering is targeted for detection. When you use URL Filtering, please set the following routing.



- The communication addressed to Server Segments targeted for detection is set so that it is routed by vFirewall to the Service Interconnect Gateway used for URL Filtering.
- The communication from the Virtual Machine is set so that it is routed by the Virtual Machine on the Server Segment targeted for detection to the Service Interconnect Gateway used for URL Filtering.
- If you perform Ping monitoring on the Virtual Machine, you will require an additional Server Segment for direct connection between vFirewall and the Virtual Machine.

INFO
- Please do not connect the Server Segments targeted for detection directly to vFirewall.

Analysis Capacity

The traffic volume that can be analyzed by URL Filtering is shown below.

Item	Performance		Remarks
	Per service	Maximum (5 services used)	
Traffic Processing Capacity	200 Mbps	1 Gbps	The total value of uplink and downlink.
Number of concurrent sessions	40,000	200,000	The number of sessions that can be connected simultaneously.

INFO
- You can increase the traffic volume up to 1 Gbps, 200,000 sessions (when 5 services used) by applying additional services.

7.4.3 Important Points

Used IP Addresses

- In order to connect the Service Interconnect Gateway with URL Filtering, you must have two IP address blocks available. If the IP address block is already being used, we might ask you to change it.
- NTT Communications will manage the assigned IP address blocks, and assign IP addresses to the devices that require them.

Restrictions

- When the actual traffic volume exceeds the contracted traffic volume, the excess traffic might be discarded.
- When the URL in Common Name of the server certificate matches the URL categorized as Block/Continue the blocking/warning screen is not displayed(it is displayed as a browser error).

- When you use a proxy server, the “Continue” action is applied only to the communication from the client (VPN) to the proxy server. It is not applied to the communication from the proxy server to the Internet from security standpoint.
- When you select “Continue” as an action for a web site categories,
  - Please add the IP address blocks of the target server segment to the proxy exception setting of a client browser. Otherwise, a warning screen will not be displayed.
  - Please set vFirewall so that the communication addressed to port 6080 of the proxy server passes through it.
  - You cannot use port 6080 for service communication which goes through URL Filtering, because port 6080 is used to display a warning screen.
- Packets which break TCP/UDP/IP protocol rules or abnormal packets are discarded as a standard function regardless of customer’s configuration.

  (Examples)
  - When the IP header is cut off in the middle
  - When the Port number is 0 (zero)
  - When the TCP flag combination is abnormal and others
- If devices making up this feature are replaced due to malfunction etc., you will not be able to check device logs or event reports from prior to the replacement via the Security Web Portal. In addition, if the regular server and the standby server are switched for a redundantly configured device and they are restored without replacing the device, you cannot check the log or the event reports for the period during which the switching occurred from the Security Web Portal.
- URL Filtering does not guarantee that the URL filtering feature has integrity or accuracy, or is suitable for your use. Furthermore, the suitability of the URL identification algorithms provided by the developers or distributors of the devices making up the URL Filtering feature is not guaranteed.
- The following information might be provided to the developers or distributors of the devices making up the URL Filtering feature.
  - Configuration information obtained from providing URL filtering
  - Information concerning controls etc., for URL filtering
- We cannot guarantee recovery from failures that might occur due to incompatibility between URL Filtering and your environment, or failures that occur due to your operations other than those specified by NTT Communications.

7.5 Application Filtering

Application Filtering is a service that blocks communication from applications that are not necessary for work, in accordance with your policies.

INFO
- Application Filtering is used via Service Interconnectivity. You need to apply separately for Service Interconnectivity.

7.5.1 Available Features

You can use the following features in Application Filtering.

Feature	Overview
Application Filtering	A feature that categorizes applications, and blocks communication from specified applications.

7.5.2 Application Filtering Feature

This feature categorizes applications by communication content, and blocks communication from specified applications.

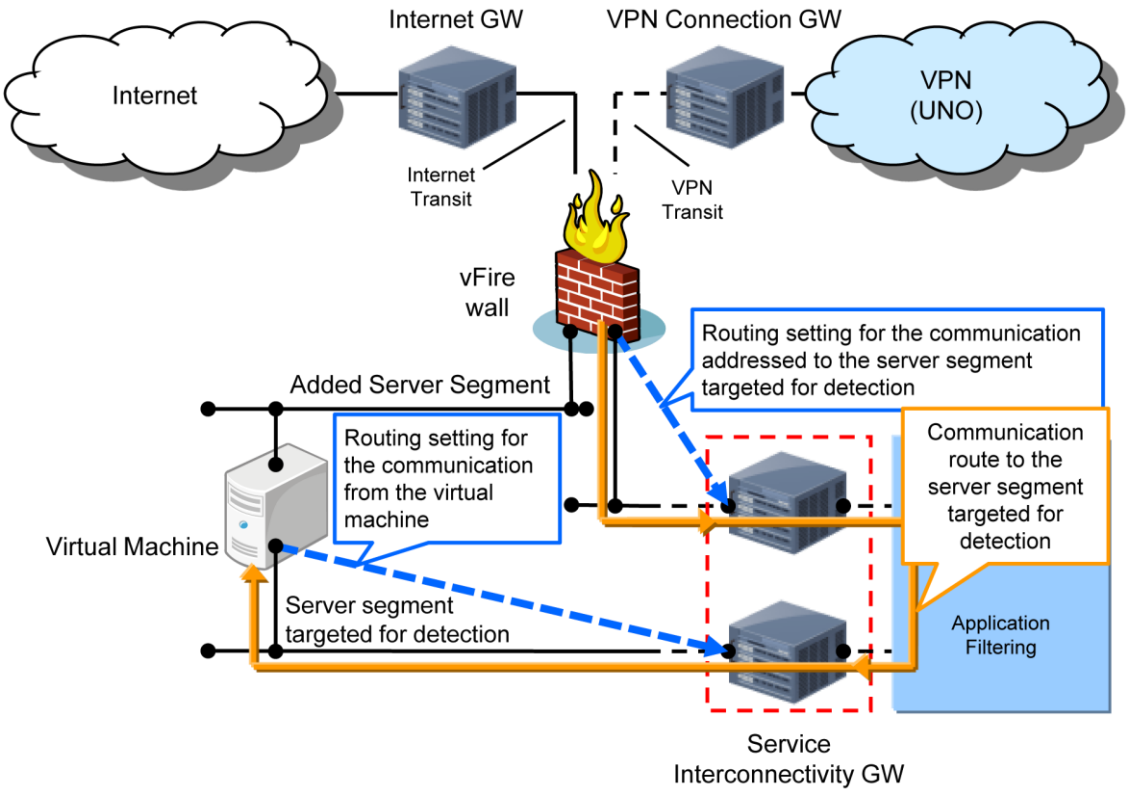
You can select applications to be blocked from among the applications that can be controlled by Application Filtering.

INFO
- Please check the following website for the controllable applications.

  http://apps.paloaltonetworks.com/applipedia/

Routing Settings

Only communication via Application Filtering is targeted for detection. When using Application Filtering, please use the following routing settings.



- The communication addressed to Server Segments targeted for detection is set so that it is routed by vFirewall to the Service Interconnect Gateway used for Application Filtering.
- The communication from the Virtual Machine is set so that it is routed by the Virtual Machine on the Server Segment targeted for detection to the Service Interconnect Gateway used for Application Filtering.
- If you perform Ping monitoring on the Virtual Machine, you will require an additional Server Segment for direct connection between vFirewall and the Virtual Machine.

INFO
- Please do not connect the Server Segments targeted for detection directly to vFirewall.

Analysis Capacity

The traffic volume that can be analyzed by URL Application Filtering is shown below.

Item	Performance		Remarks
	Per service	Maximum (5 services used)	
Traffic Processing Capacity	200 Mbps	1 Gbps	The total value of uplink and downlink.
Number of concurrent sessions	40,000	200,000	The number of sessions that can be connected simultaneously.

INFO
- You can increase the traffic volume up to 1 Gbps, 200,000 sessions (when 5 services used) by applying additional services.

7.5.3 Important Points

Used IP Addresses

- In order to connect the Service Interconnect Gateway with Application Filtering, you must have two IP address blocks available. If the IP address block is already being used, we might ask you to change it.
- NTT Communications will manage the assigned IP address blocks, and assign IP addresses to the devices that require them.

Restrictions

- When the actual traffic volume exceeds the contracted traffic volume, the excess traffic might be discarded.
- Packets which break TCP/UDP/IP protocol rules or abnormal packets are discarded as a standard function regardless of customer's configuration.

  (Examples)

  - When the IP header is cut off in the middle
  - When the Port number is 0 (zero)
  - When the TCP flag combination is abnormal and others
- If devices making up this feature are replaced due to malfunction etc., you will not be able to check device logs or event reports from prior to the replacement via the Security Web Portal. In addition, if the regular server and the standby server are switched for a redundantly configured device and they are restored without replacing the device, you cannot check the log or the event reports for the period during which the switching occurred from the Security Web Portal.
- Application Filtering does not guarantee that the Application Filtering feature has integrity or accuracy, or is suitable for your use. Furthermore, the suitability of the

application identification algorithms provided by the developers or distributors of the devices making up the Application Filtering feature is not guaranteed.

- The following information might be provided to the developers or distributors of the devices making up the Application Filtering feature.
  - Configuration information obtained from providing application filtering
  - Information concerning controls etc., for Application Filtering
- We cannot guarantee recovery from failures that might occur due to incompatibility between Application Filtering and your environment, or failures that occur due to your operations other than those specified by NTT Communications.

7.6 Web Application Firewall (WAF)

The Web Application Firewall (WAF) is a service that blocks attack traffic on Web applications.

INFO
- Web Application Firewall (WAF) is used via Service Interconnectivity. You need to apply separately for Service Interconnectivity.

7.6.1 Available Features

You can use the following features in Web Application Firewall (WAF).

Feature	Overview
Web Application Firewall	This feature detects attack traffic on Web applications, and blocks attack traffic which has a high probability of exerting a negative impact.

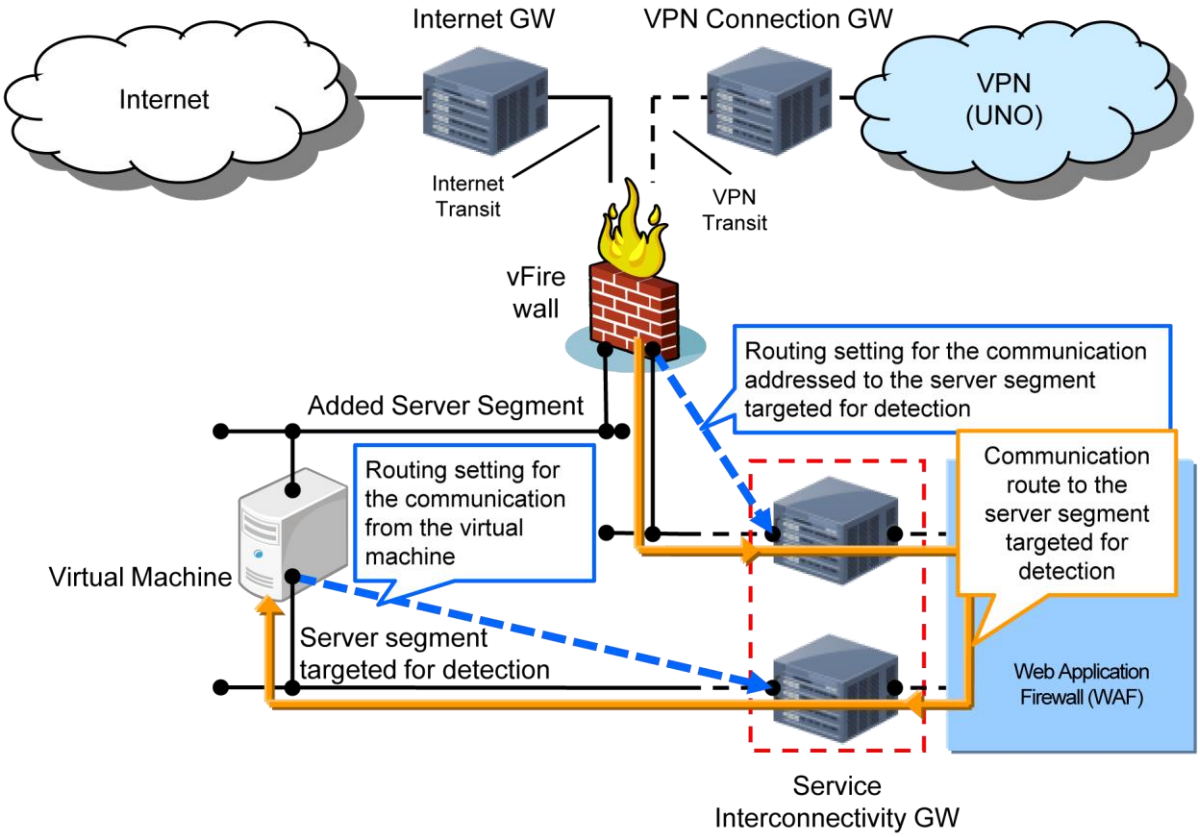
7.6.2 Web Application Firewall Feature

This feature detects attack traffic on Web applications, and blocks attack traffic which has a high probability of exerting a negative impact.

INFO
- If NTT Communications judges it necessary, we will notify you via email, etc. regarding the detection and blocking status.

Routing Settings

Only communication that goes through the Web Application Firewall (WAF) is targeted for detection. When using Web Application Firewall (WAF), please use the following routing settings.



- The communication that is addressed to the IP address block that is assigned for connecting to the Web Application Firewall (WAF) is set so that it is routed by vFirewall to the Service Interconnect Gateway used by Web Application Firewall (WAF).
- The communication from the Virtual Machine is set so that it is routed by the Virtual Machine on the Server Segment targeted for detection to the Service Interconnect Gateway used for Web Application Firewall (WAF).
- If you perform Ping monitoring on the Virtual Machine, you will require an additional Server Segment for direct connection between vFirewall and the Virtual Machine.

INFO
- Please do not connect the Server Segments targeted for detection directly to vFirewall.

Analysis Capacity

The traffic volume that can be analyzed by Web Application Firewall (WAF) is shown below.

Item	Performance (maximum value)	Remarks
Traffic Processing Capacity	1 Gbps	The total value of uplink and downlink.
RPS(Request Per Sec)	75,000 rps	-
CPS (Connection Per Sec)	10,000 cps	-

Active/Standby Structure

The Web Application Firewall (WAF) is configured in an active/standby structure. If a failure occurs in the active device, the switchover from the active device to the standby device will be performed automatically.

Staging

Staging is a process that increases the accuracy of detection and blocking of attack traffic. When you apply for Web Application Firewall (WAF), you can choose whether to implement staging. We recommend implementing it in order to reduce the amount of false positive detections.

If staging is implemented, a staging time period is set (approximately 1 – 4 weeks after you start using IPS mode) during which only detection of attack traffic is performed and traffic is not blocked. After the staging time period, please check to see whether the traffic that the Web Application Firewall (WAF) detects as being targeted for blocking is normal traffic. Based on the results of the confirmation, the Web Application Firewall (WAF) settings will be adjusted.

Policy

The policy is the defense rules in Web Application Firewall (WAF). By default, one policy is operated in Web Application Firewall (WAF). Please contact us if you would like to run more than one policy.

7.6.3 Important Points

Used IP Addresses

- In order to connect the Service Interconnect Gateway with the Web Application Firewall (WAF), you must have two IP address blocks available.
- NTT Communications will manage the assigned IP address blocks, and assign IP addresses to the devices that require them.
- When using Web Application Firewall (WAF), the following address bands cannot be used in customer networks that connect to Server Segments and Enterprise Cloud to communicate.

  172.17.62.0/24

Restrictions

- When the actual traffic volume exceeds the contracted traffic volume, the excess traffic might be discarded.
- The following health check communication is sent from devices that provide the Web Application Firewall (WAF) feature to a Virtual Machine. In the Virtual Machine settings, allow communication.
  - ICMP
  - Health check to L4 (establishing a 3-way handshake)
- Web Application Firewall (WAF) does not guarantee that the feature that detects and blocks attack traffic on Web applications has integrity or accuracy, or is suitable for your use. Furthermore, the suitability of the signatures (algorithms that judge the degree of danger and attack traffic) provided by the developers or distributors of the devices making up the Web Application Firewall (WAF) feature is not guaranteed.
- The following information might be provided to the developers or distributors of the devices making up the Web Application Firewall (WAF) feature.
  - Configuration information obtained from providing Web Application Firewall (WAF)
  - Information obtained from Web Application Firewall (WAF) controls, etc.
- We cannot guarantee recovery from failures that might occur due to incompatibility between Web Application Firewall (WAF) and your environment, or failures that occur due to your operations other than those specified by NTT Communications.

7.7 VM Anti-Virus

VM Anti-Virus is a service that defends the Virtual Machine from virus contagion and threats.

7.7.1 Available Features

You can use the following features in VM Anti-Virus.

Feature	Overview
Real-Time scan	A feature that monitors the types of file access, such as write or read, generated inside the Virtual Machine, and scans for viruses.
Scheduled scan	A feature that scans for viruses in files existing on the Virtual Machine (including files that are not in use).
Actions	A feature that executes specified processes when viruses are detected.
Scan Exception	A feature that specifies exclusion from virus scan.
Automatic Security Update	A feature that periodically checks pattern file updates and performs updates.

7.7.2 Real Time Scan Feature

The Real Time Scan feature monitors the sorts of file access, such as write or read, generated inside the Virtual Machine, and can scan for viruses.

The items that can be specified for Real Time Scan are shown below.

Item	Details
Directions and files to scan	Selects folders and files for file access monitoring. Selects the targeted folders from "All Directories," and "Directory List." Selects the targeted files from "All Files," "File types scanned by IntelliScan," and "Specified file extensions."
Target time	Selects the file access monitoring time from "24 hours a day, 365 days a year" and "Custom Schedule." If "Custom Schedule" is selected, the weekly scheduled time is specified.
Actions	For details, refer to "7.7.4 Actions" (⇒P.217).
Scan Exceptions	For details, refer to "7.7.5 Scan Exception Feature" (⇒P .219).

NOTE
- Real-time scan is only provided for the Windows OS. It cannot be used in Linux OS.

7.7.3 Scheduled Scan Feature

You can scan for viruses in files existing on the Virtual Machine (including files that are not in use) according to a specified schedule.

The items that can be specified for the Scheduled Scan Feature are shown below.

Item	Details
Directories and files to scan	Selects folders and files for file access monitoring. Selects the targeted folders from "All directories," and "Directory List." Selects the targeted files from "All Files," "File types scanned by IntelliScan," and "Specified file extensions."
Schedule	Selects the interval the scheduled scan runs from “Daily” “Weekly” or “Monthly,” and specifies the targeted time. Daily: Specifies either "Every Day," "Weekdays," or "Every X Days." Weekly: Specifies either "X day of the week each week" or "Yday of every X Weeks." Monthly: Specifies either "X day of each month" or "Every month, Y day of the week on X week."
Actions	For details, refer to "7.7.4 Actions" (->P.217).
Scan Exceptions	For details, refer to "7.7.5 Scan Exception Feature" (⇒P.219).

7.7.4 Actions

You can set the processing method for the case where files that are infected by viruses are detected.

You can specify "Recommended Setting" or "Custom Setting."

Item	Details
Recommended setting (Use action determined by ActiveAction)	The virus processing method recommended by the developers and distributors of the devices making up the VM Anti-Virus feature.
Custom setting	The first process (primary process) when viruses are detected is specified from “Delete,” “Clean,” “Pass,” “Deny access” and “Quarantine.”

INFO
- The "recommended setting" virus processing method might be modified according to day-to-day operation, and the information concerning the handling method is not disclosed.

Custom Setting

Any of the following can be specified as the first process (primary process) when viruses are detected. Note that the processing might differ depending on the Virtual Machine OS.

Item	Primary Process Details		Secondary Process Details (Process when the primary process failed)	Notification by email, etc.
	For Windows	For Linux		
Delete	The same process as "Quarantine" is performed.	The files that are infected by viruses are deleted.	The same process as "Quarantine" is performed.	Notification is made when the secondary process fails.
Clean	The viruses are removed from the files that are infected with viruses, and they return to the pre-contamination state.		The same process as "Quarantine" is performed.	Notification is made when the secondary process fails.
Pass	It is registered in the detection log. It does not take any action against the infected files.		The secondary process is not performed.	Notification is made when viruses are detected.
Deny access	During real time scanning, if some sort of file access, such as file write or read, is in a file infected with viruses, it is immediately blocked.	Real Time Scan is not supported. Access denial cannot be used.	The secondary process is not performed.	Notification is made when viruses are detected.
Quarantine	The backup data of the file that is infected with viruses is transferred to an isolation folder on the Virtual Machine, and the original file is deleted.		The secondary process is not performed.	If transfer to the isolation folder or deletion of the original file fails, notification is made.

INFO
- If "Pass" or "Deny access" is selected and the process fails, the secondary process is not executed.

7.7.5 Scan Exception Feature

By specifying directories, files and extensions, you can specify files that will not be scanned for viruses.

7.7.6 Pattern File Automatic Update Feature

This feature checks periodically for pattern file update information on NTT Communications administration server, and updates pattern files automatically if there are updates available.

Time Periods When Pattern File Automatic Updates will be run

Selects the schedule for the pattern file automatic updates, from "Daily" "Weekly" or "Monthly," and specifies the targeted time.

Item	Details
Hourly	Specifies "X minute every hour."
Daily	Specifies either "Every Day," "Weekdays," or "Every X Days."
Weekly	Specifies either "X day of the week each week" or "Yday of every X weeks."
Monthly	Specifies either "X day of each month" or "Every month, Y day of the week on X week."

7.7.7 Important Points

Virtual Machine System Requirements

The system requirements (Memory capacity, Disk capacity, and OS) for the software agent that uses VM Anti-Virus are shown below.

Item	Overview
Memory capacity	512 MB or greater
Disk capacity	1 GB or greater
OS	The OSs listed in "Supported OS List of VM Anti-Virus, VM Virtual Patch, and VM Firewall" of the available OSs in Enterprise Cloud

NOTE

- When using Linux OS, it is necessary to confirm the kernel version.
- Please set IPv6 to ON or OFF correctly when using VM Anti-Virus.

Software Agent Installation

In order to use VM Anti-Virus, upload and install agent software on the Virtual Machine. For details, refer to the agent software installation guide.

NOTE

- You cannot use the VM Anti-Virus at the same time as other anti-virus software. Before installing VM Anti-Virus agent software, always make sure to uninstall other antivirus software.
- Do not upload agents by mounting ISO image files or CD/DVD drives, when uploading it to the VMs.

INFO

- We ask you to install the agent software on the Virtual Machine.

Agent Software Default Install Location

The agent software default install location differs depending on the Virtual Machine OS.

OS	Default Install Location
Windows	C:¥Program Files¥Trend Micro¥Deep Security Agent
Linux	System files : /opt/ds_agent, /var/opt/ds_agent Startup scripts : /etc/init.d/ds_agent, /etc/init.d/ds_filter Communication channel between user and kernel mode components:/dev/dsa, /dev/dsa_ssl, /proc/driver/dsa

INFO

- You can change where it is installed. Also, the install location might change due to agent software version updates, etc.

Communication with the Manager Administered by NTT Communications

The Virtual Machine that uses the VM Anti-Virus must have communication with the Manager administered by NTT Communications.

Please set the routing and the DNS name resolution setting.

Routing Settings

- Please set the routing from the Virtual Machine to vFirewall using either of the following methods.
  - Set the Virtual Machine default gateway to vFirewall
  - Set vFirewall as the static route gateway for communication addressed to the Manager administered by NTT Communications
- If the Virtual Machine that uses VM Anti-Virus is connected to a Server Segment that is not directly connected to vFirewall, additional Server Segment is required to directly connect the vFirewall and the Virtual Machine.

DNS name resolution

In order to communicate with the Manager administered by NTT Communications, name resolution for the manager is required. Please use the DNS server inside your environment or the Virtual Machine hosts file to set name resolution for the Manager administered by NTT Communications.

Restrictions

- The following files are not targeted for virus scan.
  - Encrypted files
  - Files set with passwords
  - Corrupted files
  - Compressed files that have been compressed using unsupported formats
  - Compressed files that have been compressed six or more times in supported formats
  - Files with extracted file sizes of 10 MB or greater (real time scan default value)
  - Files with extracted file sizes of 30 MB or greater (scheduled or manual scan default value)
- You cannot set directories or files inside the network drive as targets for virus scan.
- We recommend that you do not target directories or files for virus scan that have a high write frequency, such as databases and Active Directories. If you target them for virus scan, the server performance will be reduced.
- We ask you to assume responsibility for monitoring agent software (checking to make sure it is activated at all times).
- If you use a Private Catalog to create a template of the Virtual Machine image and store it, please do it before installing the VM Anti-Virus agent software.

  If a template is created and saved from the Virtual Machine image of a Virtual Machine where VM Anti-Virus agent software is installed, or installation and activation (registration to the Manager administered by NTT Communications) is complete, when a Virtual Machine is created using that template, VM Anti-Virus can no longer be used with the Virtual Machine used for creating the template and the newly-built Virtual Machine. The same applies when used for image backup.
- VM Anti-Virus does not guarantee that the provided VM Anti-Virus feature has integrity or accuracy, or is suitable for your use. Furthermore, the suitability of the pattern files provided by the developers or distributors of the software that makes up the VM Anti-Virus feature is not guaranteed.
- The following information might be provided to the developers or distributors of the devices making up the VM Anti-Virus feature.
  - Configuration information obtained from providing VM Anti-Virus
  - Information obtained from VM Anti-Virus
- We cannot guarantee recovery from failures that might occur due to incompatibility between VM Anti-Virus and your environment, or failures that occur due to your operations other than those specified by NTT Communications.

7.8 VM Virtual Patch

VM Virtual Patch is a service that detects and protects the Virtual Machine from attacks on vulnerabilities. For OS and application vulnerabilities, it is a service that provides signatures that provide solutions equivalent to the security patches provided by application vendors.

INFO

- VM Virtual Patch uses a signature-based defense against the targeted attack traffic.
- VM Virtual Patch does not affect the performance of applications.
- VM Virtual Patch does not fix issues at the software code level, but provides temporary security measures. So please apply the regular security patches provided by each application vendor for long-term measures.

7.8.1 Available Features

You can use the following features with VM Virtual Patch.

Feature	Overview
VM Virtual Patch	A feature that detects or protects against (blocks) attack traffic directed against vulnerabilities.
Recommended scan	A feature that scans Virtual Machine system information, checks whether there are vulnerabilities, and automatically applies VM Virtual Patch corresponding to those vulnerabilities.

7.8.2 VM Virtual Patch Feature

You can choose the detection mode or the defense mode.

Mode	Overview
Detection	Attack traffic is detected. However, traffic is not blocked even though attack traffic is detected.
Defense	Attack traffic is detected. However, traffic is blocked when attack traffic is detected.

INFO

- The method for detecting attack packets is described below.

  The contents of packets that use kernel-mode drivers that are bound to L2/Data Link Layer are checked. Matching is carried out based on protocol violations and signature. Packets matching the pattern are identified as attack traffic targeting the vulnerabilities, and protective

action is taken.

- If NTT Communications judges it necessary, we will notify you via Email etc. of detection status and defense (block) status.

7.8.3 Recommended Scan Feature

It periodically scans the Virtual Machine system information, checks whether there are vulnerabilities, and automatically applies VM Virtual Patch corresponding to those vulnerabilities.

Selects the interval VM Virtual Patch are automatically applied from "Hourly" "Daily" "Weekly" or "Monthly," and specifies the targeted time.

Item	Details
Hourly	Specifies "X minute every hour."
Daily	Specifies either "Every Day," "Weekdays," or "Every X Days."
Weekly	Specifies either "X day of the week each week" or "Yday of Every X Weeks."
Monthly	Specifies either "X day of each month" or "Every month, Y day of the week on X week."

INFO

- VM Virtual Patch is effective against vulnerabilities in OS and general applications (such as apache) that are already installed.
- If you have applied a regular patch, the VM Virtual Patch will be canceled during the recommended scan.

7.8.4 Important Points

Virtual Machine System Requirements

The system requirements for operating the VM Virtual Patch agent software (Memory capacity, Disk capacity and OS) are shown below.

Item	Overview
Memory Capacity	512 MB or greater
Disk Capacity	1 GB or greater
OS	The OSs listed in "Supported OS List of VM Anti-Virus, VM Virtual Patch, and VM Firewall" of the available OSs in Enterprise Cloud

NOTE

- When using Linux OS, it is necessary to confirm the kernel version.

- Please set IPv6 to ON or OFF correctly when using VM Virtual Patch.

Agent Software Installation

In order to use VM Virtual Patch, upload and install agent software on the Virtual Machine. For details, refer to the agent software installation guide.

NOTE

- You cannot use the VM Virtual Patch at the same time as other anti-virus software than VM Anti-Virus. Before installing VM Virtual Patch agent software, always make sure to uninstall other virus protection software.
- Do not upload agents by mounting ISO image files or CD/DVD drives, when uploading it to the VMs.

INFO

- We ask you to install the agent software on the Virtual Machine.

Agent Software Default Install Location

The agent software default install location differs depending on the Virtual Machine OS.

OS	Default Install Location
Windows	C:¥Program Files¥Trend Micro¥Deep Security Agent
Linux	System files : /opt/ds_agent, /var/opt/ds_agent Startup scripts : /etc/init.d/ds_agent, /etc/init.d/ds_filter Communication channel between user and kernel mode components:/dev/dsa, /dev/dsa_ssl, /proc/driver/dsa

INFO

- You can change where it is installed. Also, the install location might change due to agent software version updates, etc.

Communication with the Manager Administered by NTT Communications

The Virtual Machine that uses the VM Virtual Patches must have communication with the Manager administered by NTT Communications.

Please set the routing and the DNS name resolution setting.

Routing Settings

- Please set the routing from the Virtual Machine to vFirewall using either of the following methods.
  - Set the Virtual Machine default gateway to vFirewall
  - Set vFirewall as the static route gateway for communication addressed to the Manager administered by NTT Communications

- If the Virtual Machine that uses VM Virtual Patch is connected to a Server Segment that is not directly connected to vFirewall, additional Server Segment is required to directly connect the vFirewall and the Virtual Machine.

DNS Name Resolution

In order to communicate with the Manager administered by NTT Communications, name resolution for the manager is required. Please use the DNS server inside your environment or the Virtual Machine hosts file to set name resolution for the Manager administered by NTT Communications.

Restrictions

- We ask you to assume responsibility for monitoring agent software (checking to make sure it is activated at all times).
- Traffic below is blocked in any mode settings.
  - TCP connections over 100,000
  - UDP connections over 100,000
  - Unusual traffic which is not based on RFC or suspected to be inaccurate.

    No IP header

    Source IP and Destination IP are the same

    Text which is not available for URI

    Using character "/" over 100

    Using "../../" above route

    And there will be blocking resulting from the shortage of compute resource.
- If you use a Private Catalog to create a template of the Virtual Machine image and store it, please do it before installing the VM Virtual Patch agent software.

  If a template is created and saved from the Virtual Machine image of a Virtual Machine where VM Virtual Patch agent software is installed, or installation and activation (registration to the Manager administered by NTT Communications) is complete, when a Virtual Machine is created using that template, VM Virtual Patch can no longer be used with the Virtual Machine used for creating the template and the newly-built Virtual Machine. The same applies when used for image backup.
- VM Virtual Patch does not guarantee that the provided VM Virtual Patch feature has integrity or accuracy, or is suitable for your use. Furthermore, the suitability of the signatures (algorithms that judge the degree of danger and attack traffic) provided by the developers or distributors of the devices making up the VM Virtual Patch feature is not guaranteed.
- The following information might be provided to the developers or distributors of the devices making up the VM Virtual Patch feature.
  - Configuration information obtained from providing VM Virtual Patch
  - Information obtained from controlling VM Virtual Patch, etc.

- We cannot guarantee recovery from failures that might occur due to incompatibility between the VM Virtual Patch feature and your environment, or failures that occur due to your operations other than those specified by NTT Communications.

7.9 VM Firewall

VM Firewall is a service that controls communication among Virtual Machines.

7.9.1 Available Features

You can use the following features with VM Firewall.

Feature	Overview
VM Firewall	A feature that controls communication among targeted Virtual Machines.

7.9.2 VM Firewall

This is a feature that specifies rules for controlling IP packets (firewall rules). It can allow or deny the passage of IP packets that match the filter conditions.

You can specify the following conditions for one control rule (firewall rule).

Item	Overview
Action Type	Specifies whether to “Allow” or “Deny” the passage of IP packets that match the conditions set by the following items.
Direction	Specifies whether the IP packets were sent from the targeted virtual machine (“Outgoing”) or are incoming IP packets (“Incoming”).
Frame Types	Specifies either "IP," "ARP," or "Other."
Protocol	For IP packet protocol, you can specify either "ICMP," "TCP" or "UDP."
Source IP Address	Specifies the source IP address of IP packets by IP address and subnet mask. You can specify multiple IP addresses or IP address ranges.
Source port number	Specifies the source port number of IP packets.
Destination IP address	Specifies the destination IP address of IP packets by IP address and subnet mask. You can specify multiple IP addresses or IP address ranges.
Destination port number	Specifies the destination port number of IP packets.

7.9.3 Important Points

Virtual Machine System Requirements

The system requirements (number of vCPU, Memory capacity, Disk capacity and OS) for operating the VM Firewall agent software are shown below.

Item	Overview
Memory Capacity	512 MB or greater
Disk Capacity	1 GB or greater
OS	The OSs listed in "Supported OS List of VM Anti-Virus, VM Virtual Patch, and VM Firewall" of the available OSs in Enterprise Cloud

NOTE
- When using Linux, it is necessary to confirm the kernel version.
- Please set IPv6 to ON or OFF correctly when using VM Firewall.

Agent Software Installation

In order to use VM Firewall, upload and install agent software on the Virtual Machine. For details, refer to the agent software installation guide.

NOTE
- You cannot use the VM Firewall at the same time as other anti-virus software than VM Anti-Virus. Before installing VM Firewall agent software, always make sure to uninstall other virus protection software.
- Do not upload agents by mounting ISO image files or CD/DVD drives, when uploading it to the VMs.

INFO
- We ask you to install the agent software on the Virtual Machine.

Agent Software Default Install Location

The agent software default install location differs depending on the Virtual Machine OS.

OS	Default Install Location
Windows	C:¥Program Files¥Trend Micro¥Deep Security Agent
Red Hat Enterprise Linux	System files : /opt/ds_agent, /var/opt/ds_agent Startup scripts : /etc/init.d/ds_agent, /etc/init.d/ds_filter Communication channel between user and kernel mode components:/dev/dsa, /dev/dsa_ssl, /proc/driver/dsa

INFO
- You can change where it is installed. Also, the install location might change due to agent software version updates, etc.

Communication with the Manager Administered by NTT Communications

The Virtual Machine that uses VM Firewall must have communication with the Manager administered by NTT Communications.

Please set the routing and the DNS name resolution setting.

Routing Settings

- Please set the routing from the Virtual Machine to vFirewall using either of the following methods.
  - Set the Virtual Machine default gateway to vFirewall
  - Set vFirewall as the static route gateway for communication addressed to the Manager administered by NTT Communications
- If the Virtual Machine that uses VM Firewall is connected to a Server Segment that is not directly connected to vFirewall, additional Server Segment is required to directly connect the vFirewall and the Virtual Machine.

DNS Name Resolution

In order to communicate with the Manager administered by NTT Communications, name resolution for the manager is required. Please use the DNS server inside your environment or the Virtual Machine hosts file to set name resolution for the Manager administered by NTT Communications.

Restrictions

- The rule names for the VM Firewall are set automatically. You cannot change the settings.
- Traffic below is blocked in any mode settings.
  - TCP connections over 100,000
  - UDP connections over 100,000
  - Unusual traffic which is not based on RFC or suspected to be inaccurate.

    No IP header

    Source IP and Destination IP are the same

    Text which is not available for URI

    Using character “/” over 100

    Using “../../” above route

    And there will be blocking resulting from the shortage of compute resource.
- We ask you to assume responsibility for monitoring agent software (checking to make sure it is activated at all times).
- If you use a Private Catalog to create a template of the Virtual Machine image and store it, please do it before installing the VM Firewall agent software.

  If a template is created and saved from the Virtual Machine image of a Virtual Machine where VM Firewall agent software is installed, or installation and activation (registration to the Manager administered by NTT Communications) is

complete, when a Virtual Machine is created using that template, VM Firewall can no longer be used with the Virtual Machine used for creating the template and the newly-built Virtual Machine. The same applies when used for image backup.

- VM Firewall does not guarantee that the provided VM Firewall feature has integrity or accuracy, or is suitable for your use.
- The following information might be provided to the developers or distributors of the devices making up the VM Firewall feature.
  - Configuration information obtained from providing VM Firewall
  - Configuration information obtained from controlling VM Firewall
- We cannot guarantee recovery from failures that might occur due to incompatibility between the VM Firewall feature and your environment, or failures that occur due to your operations other than those specified by NTT Communications.

7.10 Application Profiling

Application Profiling is a service that monitors the communication that applications are using, and provides reports that make latent risks to the applications (suspected information leaks and communication hypothesized to be unrelated to work) visible.

INFO
- Application Profiling is used via Service Interconnectivity. You need to apply separately for Service Interconnectivity.

7.10.1 Available Features

You can use the following features with Application Profiling.

Feature	Overview
Application Profiling Report	A feature that monitors the communication that applications are using, and provides reports that make latent risks to the applications (suspected information leaks and communication hypothesized to be unrelated to work) visible.

7.10.2 Application Profiling Report

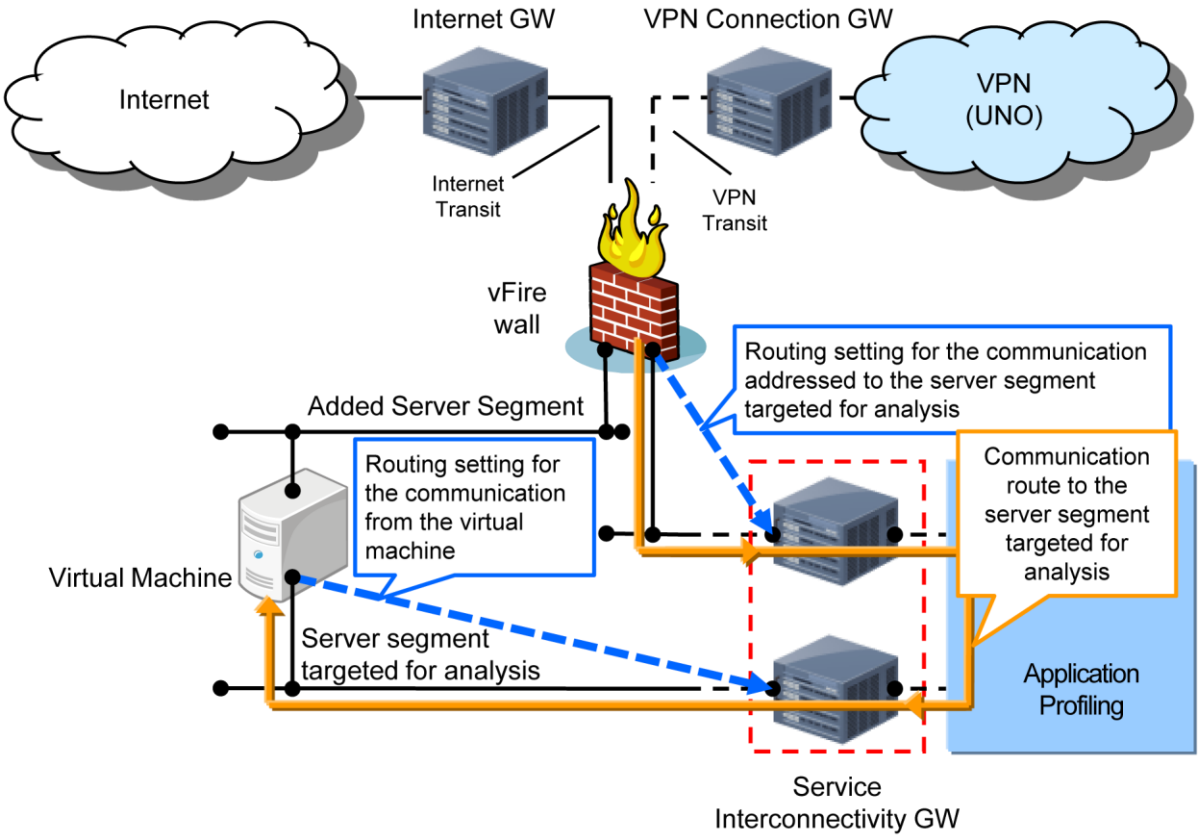
Application Profiling Report feature raises conceivable application communication that supposedly have high risk from actual application usage, displays explanations of hypothetical risks and advice for safely using the application.

INFO
- Please check the following website for the applications that can be monitored.

  http://apps.paloaltonetworks.com/applipedia/
- Reports are provided once a month.

Routing Settings

Only communication that goes through Application Profiling can be analyzed. When using Application Profiling, please use the following routing settings.



- The communication addressed to Server Segments targeted for analysis is set so that it is routed by vFirewall to the Service Interconnect Gateway used for Application Filtering.
- The communication from the Virtual Machine is set so that it is routed by the Virtual Machine on the Server Segment targeted for analysis to the Service Interconnect Gateway used for Application Profiling.
- If you perform Ping monitoring on the Virtual Machine, you will require an additional Server Segment for direct connection between vFirewall and the Virtual Machine.

INFO
- Please do not connect the Server Segments targeted for analysis directly to vFirewall.

Analysis Capacity

The traffic volume that can be analyzed by Application Profiling is shown below.

Item	Performance		Remarks
	Per service	Maximum (5 services used)	
Traffic Processing Capacity	200 Mbps	1 Gbps	The total value of uplink and downlink.

Number of concurrent sessions	40,000	200,000	The number of sessions that can be connected simultaneously.

INFO
- You can increase the traffic volume up to 1 Gbps, 200,000 sessions (when 5 services used) by applying additional services.

7.10.3 Important Points

Used IP Addresses

- In order to connect the Service Interconnect Gateway with Application Profiling, you must have two IP address blocks available. If the IP address block is already being used, we might ask you to change it.
- NTT Communications will manage the assigned IP address blocks, and assign IP addresses to the devices that require them.

Restrictions

- When the actual traffic volume exceeds the contracted traffic volume, the excess traffic might be discarded.
- Packets which break TCP/UDP/IP protocol rules or abnormal packets are discarded as a standard function regardless of customer's configuration.

  (Examples)

  - When the IP header is cut off in the middle
  - When the Port number is 0 (zero)
  - When the TCP flag combination is abnormal and others
- If devices making up this feature are replaced due to malfunction etc., you will not be able to check device logs or event reports from prior to the replacement via the Security Web Portal. In addition, if the regular server and the standby server are switched for a redundantly configured device and they are restored without replacing the device, you cannot check the log or the event reports for the period during which the switching occurred from the Security Web Portal.
- Application Profiling does not guarantee that the Application Profiling feature has integrity or accuracy, or is suitable for your use. Furthermore, the suitability of the application identification algorithms provided by the developers or distributors of the devices making up the Application Profiling feature is not guaranteed.
- The following information might be provided to the developers or distributors of the devices making up the Application Profiling feature.
  - Configuration information obtained from providing application profiling
  - Information relating to Application Profiling processing
- We cannot guarantee recovery from failures that might occur due to incompatibility between Application Profiling and your environment, or failures that occur due to your operations other than those specified by NTT Communications.

7.11 Network Profiling

Network Profiling is a service that monitors the communication to the Virtual Machine, and from the communication status provides reports that make unknown threats and latent risks visible.

INFO
- Network Profiling is used via Service Interconnectivity. You need to apply separately for Service Interconnectivity.

7.11.1 Available Features

You can use the following features with Network Profiling.

Feature	Overview
Network Profiling Report	A feature that monitors communication to the Virtual Machine and from the communication status provides reports that make unknown threats and latent risks visible.

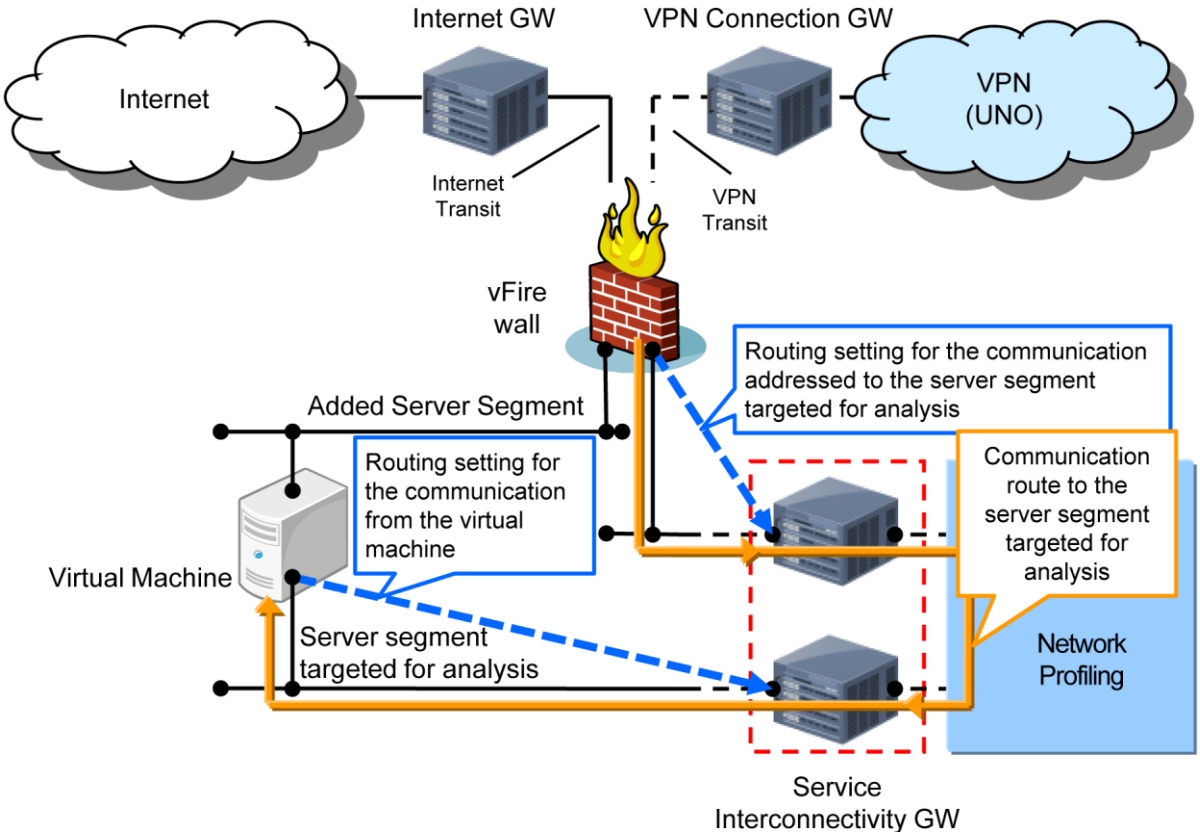
7.11.2 Network Profiling Report

It monitors communication to the Virtual Machine, and provides reports that make latent risks to the network visible, based on the correlation analyses on traffic logs and threat logs (viruses and unauthorized access) performed by a security analyst.

INFO
- Reports are provided once a month.

Routing Settings

Only communication that goes through Network Profiling can be analyzed. When using Network Profiling, please use the following routing settings.



- The communication addressed to Server Segments targeted for analysis is set so that it is routed by vFirewall to the Service Interconnect Gateway used for Network Profiling.
- The communication from the Virtual Machine is set so that it is routed by the Virtual Machine on the Server Segment targeted for analysis to the Service Interconnect Gateway used for Network Profiling.
- If you perform Ping monitoring on the Virtual Machine, you will require an additional Server Segment for direct connection between vFirewall and the Virtual Machine.

INFO
- Please do not connect the Server Segments targeted for analysis directly to vFirewall.

Analysis Capacity

The traffic volume that can be analyzed by Network Profiling is shown below.

Item	Performance		Remarks
	Per service	Maximum (5 services used)	
Traffic Processing Capacity	200 Mbps	1 Gbps	The total value of uplink and downlink.

Number of concurrent sessions	40,000	200,000	The number of sessions that can be connected simultaneously.

INFO
- You can increase the traffic volume up to 1 Gbps, 200,000 sessions (when 5 services used) by applying additional services.

7.11.3 Important Points

Used IP Addresses

- In order to connect the Service Interconnect Gateway with Network Profiling, you must have two IP address blocks available. If the IP address block is already being used, we might ask you to change it.
- NTT Communications will manage the assigned IP address blocks, and assign IP addresses to the devices that require them.

Restrictions

- When the actual traffic volume exceeds the contracted traffic volume, the excess traffic might be discarded.
- Packets which break TCP/UDP/IP protocol rules or abnormal packets are discarded as a standard function regardless of customer's configuration.

  (Examples)

  - When the IP header is cut off in the middle
  - When the Port number is 0 (zero)
  - When the TCP flag combination is abnormal and others
- If devices making up this feature are replaced due to malfunction etc., you will not be able to check device logs or event reports from prior to the replacement via the Security Web Portal. In addition, if the regular server and the standby server are switched for a redundantly configured device and they are restored without replacing the device, you cannot check the log or the event reports for the period during which the switching occurred from the Security Web Portal.
- Network Profiling does not guarantee that the Network Profiling feature has integrity or accuracy, or is suitable for your use. Furthermore, the suitability of the application, virus and URL identification algorithms provided by the developers or distributors of the devices making up the Network Profiling feature is not guaranteed.
- The following information might be provided to the developers or distributors of the devices making up the Network Profiling feature.
  - Configuration information obtained from providing network profiling
  - Information relating to Network Profiling processing
- We cannot guarantee recovery from failures that might occur due to incompatibility between Network Profiling and your environment, or failures that occur due to your operations other than those specified by NTT Communications.

7.12 RTMD Web

RTMD Web is a service that detects unauthorized malware intrusions, makes unknown threats and latent risks visible, and reports them. Principally, it provides a file analysis feature and a traffic analysis feature.

It not only performs signature-based analysis on the Customer traffic that passes through vFirewall by mirroring it, but also it actually reproduces suspicious traffic in the RTMD Web virtual environment, and analyzes malware dynamically.

INFO
- You can use one RTMD Web for every Data Center.

NOTE
- The following specification is Japan DC version. For specification of other DCs, please contact each NTT Communications affiliate.

7.12.1 Available Features

You can use the following features with RTMD Web.

Feature	Overview
File Analysis	A feature that inspects Web content that is sent and received by Web access (HTTP communication), and analyzes the content suspected of containing malware and determines whether it is malware inside the virtual environment.
Traffic Analysis	A feature that detects access to fraudulent websites, and Web access (HTTP communication) to C & C servers that is executed by malware.
Report	A feature that provides the assessment results of the file analysis and traffic analysis as daily and monthly reports.

Analysis Capacity

The traffic volume that can be analyzed by RTMD Web is shown below.

Item	Performance (maximum value)	Remarks
Traffic Processing Capacity	20 Mbps	The total value of uplink and downlink.

7.12.2 File Analysis Feature

It mirrors customer traffic that passes through vFirewall, and detects suspicious communication that might trigger an attack, such as downloads of obfuscated Java Script and executable files.

The detected communication is actually reproduced in the RTMD Web virtual environment. The content of changes generated inside the virtual environment (such as file opening, closing, creating, changing and deleting, registry changes, and API and addresses that are called) is recorded. Whether it is malware or not is determined by those results.

The Virtual Environment that Analyzes Malware

By installing operating systems (OS), Web browsers and Microsoft Office in the Malware Detection (Web) virtual environment, you can reproduce the attacks aimed at the vulnerabilities of each application, and detect malware.

You can choose from the following operating systems (OS), Web browsers and Microsoft Office versions to install in the virtual environment.

Item	Software Options
Operating System (OS)	● Windows XP ● Windows XP SP2, SP3 ● Windows 7 ● Windows 7 SP1 ● Windows 7 x64 SP1
Web Browser	● Internet Explorer 6 to 10 ● Firefox 3.5, 6.0, 17.0, 18.0, 23.0 ● Chrome 19.0, 25.0 (Windows XP, Windows 7) ● Chrome 26.0 (Windows XP)
Microsoft Office	● Microsoft Office 2003 ● Microsoft Office 2007 ● Microsoft Office 2010

7.12.3 Traffic Analysis Feature

It mirrors customer traffic that passes through vFirewall, detects access to fraudulent websites and Web access (HTTP communication) to C & C servers that is executed by malware.

INFO ● Notification of detection status is made by Email etc.

7.12.4 Report Feature

The assessment results of the file analysis and traffic analysis features are provided as daily and monthly reports. You can download the reports from the security Web portal as password-protected ZIP files.

Note that the date when downloading can start depends on the report type.

Report Type	Details	Date when downloading

		can start
Daily report	One day's worth of assessment results from the file analysis feature	From the afternoon of the day after the report target date.
Monthly report	One month's worth of assessment results from the file analysis feature	From 11 business days into the month following the report target month

INFO
- You can set a password for the ZIP files in advance.

7.12.5 Important Points

- The following files are not targeted for analysis.
  - Encrypted files
  - Files set with passwords
- Analysis may be overdue when the device limit of throughput is exceeded.
- RTMD Web cannot always be provided because it is to be inserted into the target communication route. Thus network design consideration is required before application.
- The devices that make up RTMD Web are provided in a single configuration. If the devices fail, you cannot use the RTMD Web feature. Note that there will be no effect on your usual communication.
- RTMD Web does not guarantee that the RTMD Web feature has integrity or accuracy, or is suitable for your use. Furthermore, the suitability of the signatures (algorithms that assess the degree of danger and malware) provided by the developers or distributors of the devices making up the RTMD Web feature is not guaranteed.
- The following information might be provided to the developers or distributors of the devices making up the RTMD Web feature.
  - Configuration information obtained from providing RTMD Web
  - Configuration information obtained from RTMD Web detection, etc.
- We cannot guarantee recovery from failures that might occur due to incompatibility between the RTMD Web and your environment, or failures that occur due to your operations other than those specified by NTT Communications.

7.13 RTMD Email

RTMD Email is a service that detects unauthorized malware intrusions via Email, makes unknown threats and latent risks visible, and reports them. Principally, it provides a file analysis feature.

It not only performs signature-based analysis on the Customer traffic that passes through vFirewall by mirroring it, but also it actually reproduces suspicious traffic in the RTMD Email virtual environment, and analyzes malware dynamically.

INFO
- You can use one RTMD Email for every Data Center.

NOTE
- The following specification is Japan DC version. For specification of other DCs, please contact each NTT Communications affiliate.

7.13.1 Available Features

You can use the following features with RTMD Email.

Feature	Overview
File Analysis Feature	A feature that inspects attachments to emails (SMTP communication) and URL links and analyzes the content suspected of containing malware and determines whether it is malware inside the virtual environment.

7.13.2 File Analysis Feature

It mirrors the customer traffictha‌t passes through the vFirewall, and detects suspicious files attached to email and URL links to fraudulent sites.

The attachments are actually reproduced in the RTMD Email virtual environment. The content of changes generated inside the virtual environment (such as file opening, closing, creating, changing and deleting, registry changes, and API and addresses that are called) is recorded. Whether it is malware or not is determined by those results.

The Virtual Environment That Analyzes Malware

By installing operating systems (OS), Web browsers and Microsoft Office in the Malware Detection (Email) virtual environment, you can reproduce the attacks aimed at the vulnerabilities of each application, and detect malware.

You can choose from the following operating systems (OS), Web browsers and Microsoft Office versions to install in the virtual environment.

Item	Software Options
Operating System (OS)	• Windows XP • Windows XP SP2, SP3 • Windows 7 • Windows 7 SP1 • Windows 7 x64 SP1
Web Browser	• Internet Explorer 6 to 10 • Firefox 3.5, 6.0, 17.0, 18.0, 23.0 • Chrome 19.0, 25.0 (Windows XP, Windows) • Chrome 26.0 (Windows XP)

Microsoft Office	• Microsoft Office 2003 • Microsoft Office 2007 • Microsoft Office 2010

Report Feature

The malware assessment results and the results of detection of URL links to fraudulent sites are provided in daily and monthly reports. You can download the reports from the security Web portal as password-protected ZIP files.

Note that the date when downloading can start depends on the report type.

Report Type	Details	Date when downloading can start
Daily report	One day's worth of assessment results from the file analysis feature	From the afternoon of the day after the report target date.
Monthly report	One month's worth of assessment results from the file analysis feature	From 11 business days into the month following the report target month

INFO • You can set a password for the ZIP files in advance.

Analysis Capacity

The traffic volume that can be analyzed by RTMD Email is shown below.

Item	Performance (maximum value)
Number of emails	150,000 emails/day (6,250 emails per hour)
Number of email accounts	100 email accounts

7.13.3 Important Points

- The following files are not targeted for analysis.
  - Encrypted files
  - Files set with passwords
- Analysis may be omitted when the device throughput limit is exceeded.
- RTMD Email cannot always be provided because it is to be inserted into the target communication route. Thus network design consideration before application is required.
- The devices that make up RTMD Email are provided in a single configuration. If the devices fail, you cannot use the RTMD Email feature. Note that there will be no effect on your usual communication.
- RTMD Email does not guarantee that the RTMD Email feature has integrity or accuracy, or is suitable for your use. Furthermore, the suitability of the signatures (algorithms that assess the degree of danger and malware) provided by the developers or distributors of the devices making up the RTMD Email feature is not guaranteed.
- The following information might be provided to the developers or distributors of the devices making up the RTMD Email feature.
  - Configuration information obtained from providing RTMD Email
  - Configuration information obtained from RTMD Email detection, etc.
- We cannot guarantee recovery from failures that might occur due to incompatibility between the Real Time Malware Detection (Email) and your environment, or failures that occur due to your operations other than those specified by NTT Communications.

8. Maintenance and Operation of the Enterprise Cloud (Japan Contract)

At the NTT Communications Support Center, our highly skilled staff support stable operations 24 hours/365 days.

8.1 Set of Materials Sent When You Start Using the Service

When you start using Enterprise Cloud, we will send you the following documents.

All services	Commencement information

8.2 Customer Support

8.2.1 Support Center/Technical Help Desk

If you think there has been a failure or you do not understand how to configure the system, contact the following center that is appropriate for your situation.

Inquiries regarding a failure	Support Center
Technical inquiries	Technical Help Desk

INFO

- Please refer to the commencement information for contact details.
- To use the Support Center or Technical Help Desk, you will need your "customer number" that is provided when you start the service.
- The scope of support is limited to inquiries relating to the contracted service.

Ticket function

Ticket can be send by Customer Portal. But ticket function cannot be used when there is no contract of Data Center within the region to which Customer's country belongs. (For example contract in Japan using only Singapore Serangoon Data Center.)

Region	Contract	Data Center Name
Japan	Japan	Yokohama No.1 Data Center Kansai1 Data Center Saitama No.1 Data Center
	Hong Kong	Hong Kong Tai Po Data Center
US	US	San Jose Lundy Data Center Virginia Sterling Data Center
UK	UK	Hemel Hempstead2 Data Center
	Germany	Frankfurt2 Data Center
APAC	Singapore	Singapore Serangoon Data Center
	Malaysia	Malaysia Cyberjaya3 Data Center
	Thailand	Thailand Bangna Data Center
	Australia	Australia Sydney1 Data Center

The priority of the tickets will be judged according to its content.

Due to this, the response to the tickets may not be in order when there are several tickets opened.

Incident Management

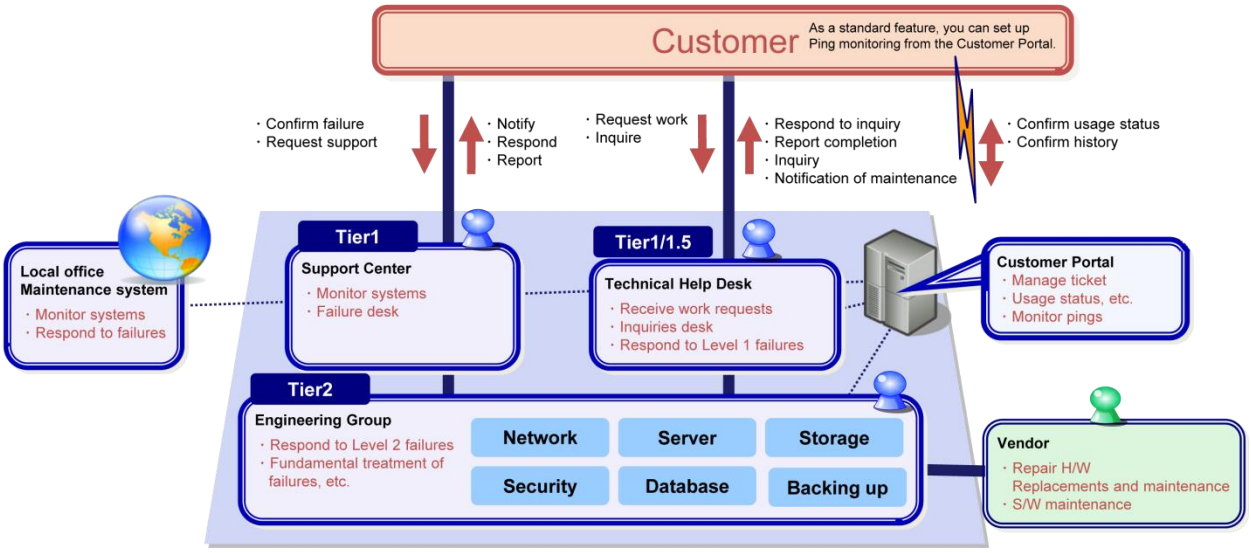
The following matters are treated as "incidents." All "incidents" are managed using a ticket system and are assigned a "ticket number" in the Customer Portal.

- Inquiries and requests notified to the Support Center or Technical Help Desk
- If the matter is outside of the threshold of monitored items stipulated for each service,

  the failure will be handled promptly as required.

8.2.2 Maintenance and Operations System

An overall diagram of maintenance and operations at NTT Communications is shown below.



8.3 Contact When a Failure Occurs

When a failure is detected or an alert is generated in the Enterprise Cloud, you will be notified by the Support Center.

You will be notified through one of the following methods. The notification methods are different for each service.

Notification Procedure	Overview
L1	Notified by telephone and email and displayed in the Customer Portal 24 hours, 365 days.
L2	Notified by email and displayed in the Customer Portal 24 hours, 365 days. Also notified by telephone during business hours (if a failure occurs outside of business hours, you will be notified by telephone the following business day). ※ Business hours are 10:00 a.m. to 5:00 p.m. (JST) (1:00 a.m. to 8:00 a.m. (UTC)) weekdays.
L3	Notified by email and displayed in the Customer Portal 24 hours, 365 days.
L4	Displayed in the Customer Portal.

INFO

- NTT Communications will determine whether to contact you when performance declines.

8.3.1 Items Monitored Remotely and Procedures for Notifying Users

Monitoring targets and customer notification methods differ for each service.

Service	Monitoring Procedure	Interval (Seconds)	Monitoring Target	Notification Procedure
Compute Resource	Ping	60	Primary vNIC for Virtual Machines	L4 (※1)
vFirewall	Ping	60	Server Segment-side Network Interface	L4
vLoad Balancer	Ping	60	IP address for the Server Segment connection	L4
Service Interconnectivity	Ping	60	Server Segment-side Network Interface	L4
VPN Connectivity	Ping	60	Network interface on the VPN Transit side	L4
Internet Connectivity	Ping	60	Network interface on the Internet Transit side	L4
Colocation Interconnectivity	Link UP/Down	Always	Network interface for colocation interconnectivity on NTT Communications' equipment	L3 (※2)
On-Premises Interconnectivity	Ping	60	Network interface for internet at the on-premises connectivity gateway in Data Centers and the on-premises connectivity gateway on premise.	L3 (※2)
Global File Storage (Global Data Backup)	Ping and SNMP Trap	60	Primary Storage	-

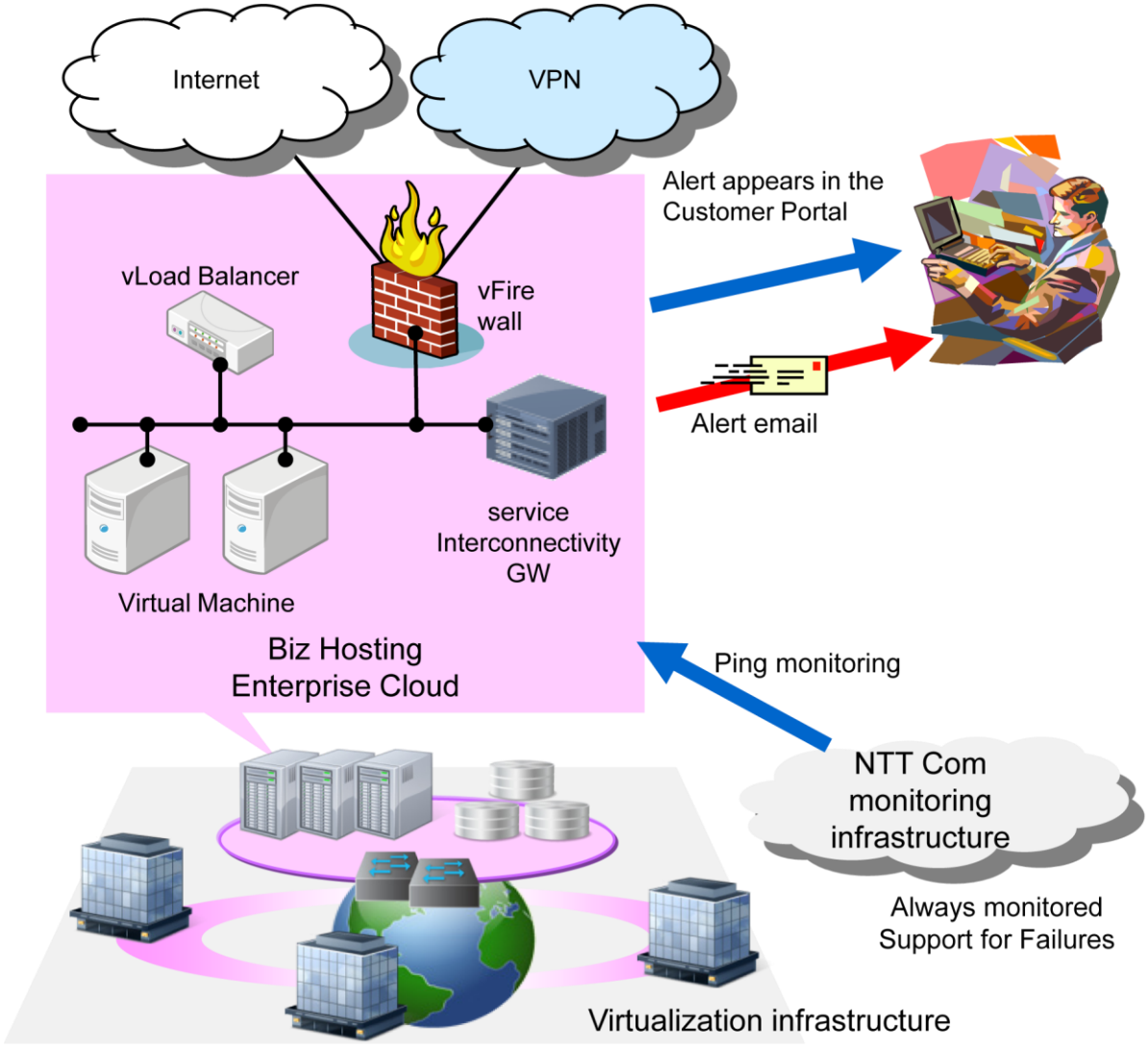
※1 Customer Portal features can be used to send an alarms from ping monitoring infrastructure to a pre-specified email address.

※2 This is an email notification only. It is not displayed in the Customer Portal.

8.3.2 Remote Monitoring System

In the Enterprise Cloud, the NTT Communications monitoring infrastructure monitors your contracted resources 24 hours, 365 days.

A diagram of the Enterprise Cloud monitoring is shown below.



Ping Monitoring for Compute Resource

Ping monitoring settings

If you set up monitoring notifications from the Customer Portal, you can perform Ping monitoring on Compute Resource. Also, using the Customer Portal you can set the alarm notification setting On/Off for each virtual server whenever the Virtual Machine is powered on.

Ping monitoring contents

The primary vNICs of Virtual Machines created in a Compute Resource Pool are pinged by the NTT Communications monitoring infrastructure every 60 seconds.

If the ping fails three times in a row, a notification is sent to the registered email address and displayed in the Customer Portal. If after that Ping succeeds even one time, it is judged to be recovered, and the alarm notification is stopped.

Ping Monitoring of the vFirewall, vLoad Balancer, Service Interconnectivity, VPN Connectivity, and Internet Connectivity

The network interface for monitored devices is pinged by the NTT Communications monitoring infrastructure every 60 seconds.

If the ping fails three times in a row, a notification is displayed in the Customer Portal. If after that Ping succeeds even one time, it is judged to be recovered, and the alarm notification is stopped.

Ping Monitoring of On-Premises Interconnectivity

The monitored network interfaces are pinged by the NTT Communications monitoring infrastructure every 60 seconds.

If the ping fails three times in a row, a notification is sent to the registered email address. If after that Ping succeeds even one time, it is judged to be recovered, and the alarm notification is stopped.

Monitoring Infrastructure Equipment

NTT Communications will monitor the infrastructure equipment making up the Enterprise Cloud.

If a failure occurs on your dedicated infrastructure equipment or infrastructure equipment for NTT Communications services that affect multiple customers, a notification is sent to all customers that may be affected. A detailed report is not necessarily included in the notification details.

INFO

- If a partial failure occurs that does not affect your use of the system, we may perform maintenance work without sending you a notification.

8.4 Maintenance Information

In the Enterprise Cloud, we perform the maintenance necessary for continuous use of your system, as required. The primary maintenance is described below.

- Taking countermeasures against security vulnerability
- Maintenance work and improvements on server and network devices

Advance Notice

If there are plans to perform maintenance, the Technical Help Desk will typically post maintenance information on the Customer Portal two weeks in advance (unless the work is urgent).

INFO

- The maintenance information may include a request to borrow your system.
- If a partial failure occurs that does not affect your use of the system, we may perform maintenance work without sending you a notification.
- The switching behavior for devices in a redundant configuration at the time of a failure of active device or the interface for the active device is an automatic switch to a standby device. However, you may need to manually switch from the standby device back to the active device when the active device recovers.

8.5 Limitations to Maintenance Operations

Support for Failures

When handling failures, we may have no choice but to restore your system to the state it was in when you started using the Enterprise Cloud.

Ping Monitoring

- You cannot instruct us to stop ping monitoring on your Virtual Machine.
- Monitoring cannot be performed when the primary vNIC is connected to a Server Segment that is not connected to vFirewall.
- When adding a Server Segment, you can perform ping monitoring for each device connected to this Server Segment by connecting this Server Segment to vFirewall.
- Changing the settings on your Guest OS may cause pings to fail if response packets from the primary vNIC are lost. This may be interpreted as a ping error.

Definition of Weekdays/Business Days

Weekdays/business days are based on Japan Standard Time (JST). They are Monday to Friday, except for national holidays stipulated under the laws of Japan, and the New Year period as stipulated by NTT Communications (December 29 to January 3).

Index

A

Application Filtering 210

Application Profiling 232

B

Backup 116, 187

C

Colocation Interconnectivity 150

Compute 52

Compute Resource 52

Compute Resource (Dedicated Device) 75

Contact When a Failure Occurs 247

Customer Portal 41

Customer Support 245

Customer System Environment 154

D

Database License 98

Database License (MS SQL) 98

Detection and blocking of attack traffic . 194, 224

Detection and blocking of unauthorized access 194

E

Email-Anti-Virus 198

Enterprise Cloud Customer Portal 41

Equipment Environment 18

Example Usage Model 35

External Storage Feature 187

F

Firewall 160, 214, 228

G

Global Data Backup 187

Global File Storage 187

Global IP Address 132

Global Standard Menu 14

Guest OS Customization 67, 68

I

Image Backup 116

Internet Connectivity 132

IPS/IDS 194

Items Monitored Remotely and Procedures for Notifying Users 248

L

Load Balancer 166

Load Distribution 166

Local Option Menu 33

M

Maintenance and Operation (Japan Contract) 244

Maintenance and Operations 252

Maintenance and Operations System 246

Maintenance Information 251

Malware Detection (Email) 240

Malware Detection (Web) 238

Microsoft SAL 113

Microsoft SQL Server License 98

N

NAT/NAPT Feature 160

Network Features 132

Network profiling 235

O

On-Premises Interconnectivity 154

OS License 93

Overview 10

P

Packet Filtering Feature 160

Virtual 224

Portal Site 41

Private Catalog 88

R

RDS SAL 113

Real Time Malware Detection (Email) 240

Real Time Malware Detection (Web) 238

Red Hat Enterprise Linux 93

Remote Monitoring System 249

Routing Feature 160

S

Security Features 194

Security Web Portal 47

Server Segment 141

Service Interconnectivity 146

Service Management 41

Set of Materials Sent When You Start Using the Service 244

Support Center 245

T

Technical Help Desk 245

Template 88

Terms 37

V

vFirewall 160

Virtual Machine 88

vLoad Balancer 166

VM-Anti-Virus 218

VM-Firewall 228

VPN Connectivity 136

W

WAF 214

Web Application Firewall 214

Web-Anti-Virus 202

Windows Server 93

[Revision History]

Date Updated	Version No.	Revision Details
04/05/2013	Ver.1.00	Ver.1.00 established
04/26/2013	Ver.1.10	1) Changed the name of a menu New Compute Resource (Dedicated Device) Old Dedicated Cluster 2) Added a storage class (Premium +) to Compute Resource (Dedicated Device) 3) Added database license (MS SQL) 4) Added a menu that can only be used at Japan Data Centers 5) Fixed other notation variations
06/03/2013	Ver.1.11	1) Added a note about the number of vLoad Balancer sessions 2) Fixed typographical errors
06/10/2013	Ver.1.12	1) Fixed the diagram of the equipment environment 2) Fixed the list of features shared between portals 3) Fixed an error in the UKDC name
07/18/2013	Ver.1.2	1) Added On-Premises Interconnectivity 2) Added image backup 3) Added the IP address management feature for Server Segments
09/05/2013	Ver.1.21	1) Added Single Sign-On
09/25/2013	Ver.1.3	1) Added security 2) Added Remote Client Connection 3) Fixed Data Center availability 4) Other minor corrections
10/07/2013	Ver.1.31	1) Remote Client Connection Fixed terminal-type delivered addresses
11/15/2013	Ver.1.4	1) Added the Disk extension feature for Virtual Machines 2) Added the wide-band plan for VPN Connectivity and Internet Connectivity 3) Provided the separate releases for vFirewall and vLoad Balancer 4) Added Colocation Interconnectivity 5) Added global file storage (Global Data Backup) and the feature for restoring from secondary storage
12/10/2013	Ver.1.5	1) Added RDS SAL 2) Fixed Colocation Interconnectivity

		3) Fixed security
7/1/2014	Ver.2.12	1) Added Integrated Network appliance 2) Added Colocation Interconnectivity 3) Added Guaranteed Compute 4) Added Dedicated Compute (S/M/L) 5) Updated Security Option Menu 6) Updated the table "Service Provided by Each Data Center"
8/1/2014	Ver.2.13	1) Delete Important Point about OS License activation in case of using Integrated Network Appliance. 2) Updated service menu list in each Data Center. 3) Updated Security Service. 4) Delete Important Point about contract in Colocation Connectivity.
8/20/2014	Ver.2.14	1) Updated OS Lisence (Windows Server 2012) 2) Updated important point in Internet Connectivity. (The DNS resolver is not offered with this service.)
9/1/2014	Ver.2.15	1) Updated Image Backup 2) Added File Backup 3) Updated service menu list in each Data Center. 4) Updated IPsec parameters in Integrated Network Appliance 5) Updated Security
9/5/2014	Ver.2.16	1) Updated service menu list in each Data Center. 2) Updated Security
9/12/2014	Ver.2.17	1) Added OS Lisence (Windows Server 2012) in US,MY 2) Updated File Backup
10/1/2014	Ver.2.18	1) Updated service menu list in each Data Center. 2) Updated Japanese local service menu. 3) Updated Customer Portal function. 4) Updated VPN Connectivity and Server Segment. 5) Updated Colocation Connectivity.
11/12/2014	Ver.2.19	1) Updated service menu list in each Data Center INA (US/UK/Kansai), Security Option 2) Updated Image Backup 3) Updated Server Segment 4) Updated Database License OS template version for Windows Server 2012 5) Updated Security Option (URL Filtering) 6) Updated Ticket Function
12/9/2014	Ver2.20	1) Updated the All Service Specifications related to Germany DC as it is now aligned with other DCs 2) Revised Compute Resource (Dedicated) Deleted the description regarding the Customer Portal

		management of the Compute Resource. 3) Updated OS Licence Added Windows Server R2 template 4) Updated Image Backup vNIC bugfixed in restore for Windows Server 2012 5) Updated File Backup Corrected the job slot time 6) Updated Server Segment Added description on Customer's carried-in Global IP
12/26/2014	Ver2.21	1) Updated service menu list in each Data Center Guaranteed Compute (TH) 2) Updated OS License Windows Server R2 template (available in JP DC(Yokohama), MY, TH) 3) Updated Image Backup 4) Updated "8.3.1 Items Monitored Remotely and Procedures for Notifying Users" Ping Monitoring is available in Integrated Network Appliance
1/7/2015	Ver2.211	1) Revision in Integrated Network Appliance IPsec Termination Parameter (Key management protocol) P.181 wrong:IKEv2(ISAKMP+Oakley) correct:IKEv1(ISAKMP+ Oakley)
1/19/2015	Ver2.23	1) Updated Customer Portal ver2.0 2) Updated service menu list in each Data Center Added: Saitama No,1 Datacenter 3) Updated Compute Resource Updated Assigning Resources to a Virtual Machine (Both Shared and Dedicated Compute) 4) Updated Private Catalog Added restrictions of VM size for creating template 5) Updated Database License Added restrictions for configurable value. 6) Updated Image Backup Added description for Supported VM size
2/27/2015	Ver2.34	1) Updated service menu list in each Data Center 2) Updated Compute Resource Memory overhead parameters for vCPUs/Guest OS Customization period:from 10 minutes to 30 minutes 3) Updated OS License Added Windows Server 2012/R2 in SG

		4) Updated Server Segment 24 can be available in INA. Maximum Server Segments which can connect to INA are up to 7. DNS suffix can be specified by Customer 5) Updated vLoad balancer (Updated restriction for using Cookie Insert Method or x-forwarded-for header addtion)
3/10/2015	Ver2.35	1) Updated Customer Portal Version List Ver2.0 is available in Saitama No.1 Data Center 2) Updated Filebackup Important Points
3/23/2015	Ver2.36	1) Updated OS License Windows Server 2012/R2 is available in AU 2) Updated Customer Portal Version List Ver2.0 is available in UK 3) Updated service menu list in each Data Center Guaranteed Compute is available in AU 4) Updated Colocation Connectivity Kyoto No.2 Data Center is available in Kansai1 Data Center